

**RANCANG BANGUN FITUR CACTI BERBASIS *SHORT
MESSAGES SERVICE* UNTUK PENYAMPAIAN
NOTIFIKASI MASALAH JARINGAN DENGAN *PRIORITY
SERVICE***

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik Pada
Jurusan Teknik Informatika

Oleh :

EKY RAHAYU ARISANTI
10451025516



**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2010**

Laporan Tugas Akhir dari Samping

TUGAS AKHIR

**Rancang Bangun Fitur Cacti berbasis *Short Messages Service* untuk Penyampaian
Notifikasi Masalah Jaringan dengan *Priority***

EKY RAHAYU ARISANTI

10451025516



2010

RANCANG BANGUN FITUR CACTI BERBASIS *SHORT MESSAGES SERVICE* UNTUK PENYAMPAIAN NOTIFIKASI MASALAH JARINGAN DENGAN *PRIORITY SERVICE*

EKY RAHAYU ARISANTI
10451025516

Tanggal Sidang : 15 Februari 2010
Periode Wisuda : Juli 2010

Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Monitoring jaringan berguna untuk memantau informasi statistik jaringan untuk pencegahan masalah jaringan, ataupun untuk mengetahui masalah jaringan yang sedang terjadi sehingga penanganannya dapat dilakukan secepat mungkin. CACTI adalah *tools* monitoring jaringan yang dapat merekam statistik jaringan berdasarkan konsep SNMP dan mengirimkan pesan peringatan bila terjadi masalah di jaringan dalam bentuk *email*. Namun, email pada CACTI memiliki kekurangan dalam hal waktu akses karena menyertakan grafik hasil monitoringnya.

Dalam tugas akhir ini dibangun sebuah fitur yang dapat melengkapi dan menutupi kekurangan pada fitur CACTI. Fitur tersebut akan diintegrasikan dengan teknologi SMS dan metode *priority service* untuk memberitahukan masalah yang terjadi di jaringan, sehingga masalah yang ada dapat ditangani secepatnya. Konsep kerjanya adalah pada saat CACTI menangkap adanya masalah jaringan, laporan mengenai hal tersebut akan dikirim secara langsung melalui SMS berdasarkan prioritas yang telah ditentukan.

Hal yang dilakukan adalah menginstal dan menganalisa CACTI, merancang proses integrasi SMS dan metode *priority service* pada CACTI, mengimplementasikannya dengan bahasa pemrograman PHP dan MySQL serta melakukan uji coba dengan perangkat jaringan yang ada. Tugas akhir ini menghasilkan fitur CACTI yang mampu memberikan notifikasi berupa SMS tentang masalah yang terjadi di jaringan dengan keunggulan pengiriman SMS yang otomatis dan penentuan kategori masalah jaringan yang dinamis.

Kata Kunci: CACTI, *Priority Service*, SMS

DESIGN AND IMPLEMENTATION OF CACTI'S FEATURE SMS BASED TO SEND ALERT OF NETWORK PROBLEM USING PRIORITY SERVICE

EKY RAHAYU ARISANTI
10451025516

Final Exam Date : February 15th, 2010
Graduation Ceremony Period : July , 2010

Informatics Engineering Department
Faculty of Sciences and Technology
State Islamic University of Sultan Syarif Kasim Riau

ABSTRACT

Network monitoring is used to collect network statistic in order to prevent network problem, or to record network problems currently so the network troubleshooting can be done as soon as possible. CACTI is a network monitoring tool that can collect and record network statistics based on the concept of SNMP network and send alert via email when the network is in trouble. But email has disadvantages in term of its access time because CACTI embeded graphics in it.

This final task develop a feature that can complete CACTI's feature. This feature will be integrated with SMS technology and priority service method to give alert of network problems, so that the network problems can be fixed as soon as possible. The concept is, CACTI will record the network problems and the feature will be sends alert immediately based on the priority that has been define before.

To do in this final task are installing and analyzing CACTI, designing how to integrate SMS and priority service into CACTI, implementing by using PHP and MySQL languages and testing into some network device. The result of this final task is CACTI's feature that can be used to give notification of network problems via SMS, with the advantages SMS sent automatically and it has a dynamic feature in defining the network problems.

Keywords: CACTI, Priority Service, SMS

DAFTAR ISI

	Halaman
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL	iv
LEMBAR PERNYATAAN	v
LEMBAR PERSEMBAHAN	vi
ABSTRAK	vii
<i>ABSTRACT</i>	viii
KATA PENGANTAR	ix
DAFTAR ISI	xii
DAFTAR GAMBAR	xv
DAFTAR TABEL	xix
DAFTAR LAMPIRAN	xxi
BAB I PENDAHULUAN	I-1
1.1 Latar Belakang	I-1
1.2 Rumusan Masalah	I-5
1.3 Batasan Masalah	I-5
1.4 Tujuan Penelitian	I-6
1.5 Sistematika Penulisan	I-7
BAB II LANDASAN TEORI	II-1
2.1 Analisa Kinerja Jaringan	II-1
2.1.1 Kategori dan Tujuan	II-2
2.1.2 Parameter Kinerja Jaringan	II-2
2.1.3 SNMP sebagai Indikator Kinerja Jaringan (Utilization) ..	II-3
2.2 Standar Keamanan Jaringan dan Contoh Permasalahan	II-7
2.3 Manajemen Jaringan	II-14
2.3.1 <i>Simple Network Management Protocol (SNMP)</i>	II-14
2.3.2 Konsep SNMP	II-14
2.3.3 <i>Management Information Bases (MIBs)</i>	II-17
2.3.4 Arsitektur SNMP	II-17

2.3.5	Protokol SNMP	II-18
2.3.6	Perkembangan SNMP	II-19
2.4	CACTI	II-21
2.4.1	Data Source.....	II-22
2.4.2	Graph (Grafik dalam CACTI)	II-22
2.4.3	<i>User management</i> (Manajemen Pengguna).....	II-23
2.4.4	<i>Templating</i>	II-23
2.5	SMS	II-27
2.5.1	Pengertian SMS	II-27
2.5.2	Fasilitas Dasar SMS	II-27
2.5.3	Prototokol Data Unit.....	II-28
2.6	Teori antrian	II-29
2.6.1	Komponen Dasar Antrian.....	II-30
2.6.2	Sistem Antrian dengan menggunakan Prioritas Pelayanan (<i>priority service</i>)	II-32
2.7	Now SMS	II-33
BAB III METODOLOGI PENELITIAN		III-1
3.1	Siklus Hidup Pengembangan Sistem	III-1
3.2	<i>System Development methodology</i>	III-5
3.2.1	Functional Decomposition methodologies	III-5
3.2.2	<i>Data Orientied methodologies</i>	III-5
3.3	Analisa Kebutuhan Sistem	III-7
3.3.1	Kebutuhan Perangkat keras (<i>Hardware</i>).....	III-7
3.3.2	<i>Software Requirements</i> (Kebutuhan Perangkat Lunak).....	III-7
3.4	Perancangan	III-8
3.5	Implementasi dan Pengajian.....	III-9
3.6	Analisis Akhir	III-9
BAB IV ANALISA DAN PERANCANGAN		IV-1
4.1	Analisa Sistem Yang Sedang Berjalan	IV-1
4.2	Analisa Sistem yang Akan Dibangun.....	IV-5

4.2.1	Analisa Permasalahan CACTI tanpa fitur SMS	IV-5
4.2.2	Analisa Penggunaan Priority Service dalam (FiturCACTI berbasis SMS).....	FiCtiMS IV-8
4.2.3	Deskripsi Umum Sistem yang akan Dibangun.....	IV-13
4.2.4	Analisa Perangkat Lunak.....	IV-16
4.3	Perancangan Sistem.....	IV-24
4.3.1	Perancangan Basis Data.....	IV-25
4.3.2	Perancangan Antar Muka	IV-28
BAB V IMPLEMENTASI DAN PENGUJIAN.....		V-1
5.1	Implementasi Sistem	V-1
5.1.1	Alasan Pemilihan Perangkat Lunak.....	V-2
5.1.2	Lingkungan Implementasi	V-2
5.1.3	Hasil Implementasi	V-5
5.2	Pengujian Sistem	V-9
5.2.1	Kebutuhan Perangkat Uji Coba dan Pengujian	V-10
5.2.2	Pengujian Proses Login pada CACTI FiCtiMs	Sekaligus V-13
5.2.3	Pengujian Pendaftaran Host pada CACTI.....	V-15
5.2.4	Pengujian Pendaftaran Host pada Thold	V-18
5.2.5	Pengujian FiCtiMS	V-19
5.2.6	Kesimpulan Hasil Pengujian	V-22
BAB VI PENUTUP.....		VI-1
6.1	Kesimpulan.....	VI-1
6.2	Saran	V-2
DAFTAR PUSTAKA		
LAMPIRAN		

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi jaringan komputer telah berkembang sangat pesat dalam waktu yang cukup singkat. Dengan makin berkembangnya teknologi saat ini maka sistem komputer tidak lagi digunakan untuk kebutuhan sendiri (*personal use*) melainkan untuk keperluan banyak pihak melalui suatu struktur jaringan/ *network*. Saat ini jutaan sampai milyaran komputer telah terhubung satu sama lainnya, baik dalam jaringan lokal, regional, nasional bahkan internasional. Seiring itu pula, manajemen yang baik terhadap suatu sistem jaringan sangat diperlukan, agar pemanfaatannya berjalan lancar dan terus menerus sehingga dapat memenuhi berbagai kebutuhan pengguna.

Manajemen jaringan terdiri dari pemantauan, pengontrolan dan perencanaan terhadap sistem atau sumber daya jaringan komputer (Terplan, 1992). Pemantauan merupakan kegiatan yang dilakukan oleh seorang administrator jaringan untuk memelihara atau menjaga agar sistem dan sumber daya jaringan dapat berjalan lancar. Dengan adanya pemantauan, informasi mengenai komponen jaringan yang meliputi *hardware*, *software*, penanggung jawab, lokasi dan nama masing-masing *workstation* dapat secara jelas diketahui. Selain itu, manajemen jaringan komputer semakin diutamakan untuk menjaga integritas dan lebih terstrukturnya jaringan yang dibangun.

Informasi mengenai statistik kinerja jaringan merupakan hal yang sama pentingnya dengan jaringan itu sendiri. Oleh karena itu, seorang administrator

jaringan harus mampu memastikan mana *workstation* yang dapat digunakan atau terhubung ke jaringan dan mana yang tidak sehingga masalah pada jaringan dapat diketahui lebih awal dan perbaikan akan adanya kerusakan pada jaringan dapat dilakukan sedini mungkin, tanpa harus mengabaikan aspek biaya dan waktu.

Lazimnya, proses monitoring jaringan dilakukan secara rutin dengan pengecekan dan pencatatan kondisi jaringan secara manual. Beberapa fasilitas yang biasa digunakan adalah *ping* pada sistem operasi. Kelemahan dari cara monitoring seperti ini adalah ia hanya memberitahu bahwa di suatu tempat antara stasiun monitoring dan perangkat target terdapat gangguan komunikasi. Gangguan bisa jadi router, switch, atau bagian jaringan lainnya yang tidak baik, atau memang *host*-nya yang sedang *down*. Tes ping hanya mengatakan bahwa koneksi *down*, tidak di mana terjadinya *down*.

Untuk sebuah jaringan (*network*) berskala besar, hal seperti diatas tidak mungkin diterapkan karena dari segi analisa biaya dan waktu, hal tersebut memerlukan sumber daya (*resource*) yang besar. Oleh sebab itu, tugas akhir ini dibuat untuk memberikan solusi agar kondisi statistik jaringan dapat dikumpulkan dan diatur pada satu lokasi sentral, yang artinya akan diimplementasikan suatu aplikasi manajemen jaringan yang mampu melakukan pemantauan secara terpusat dan menjangkau seluruh host pada jaringan.

Umumnya jam kerja seorang administrator jaringan tidak lebih dari 8 jam setiap harinya. Sementara keberlangsungan bisnis (*bussiness continuity*) yang ditangani suatu jaringan harus tetap terjaga. Oleh sebab itu, sangatlah diperlukan suatu sistem yang mampu memonitoring aktifitas jaringan selama 24 jam penuh

sekaligus terintegrasi dengan alat yang mampu memberikan notifikasi saat ketersediaan akses ke jaringan sedang terputus. Dengan demikian meskipun seorang administrator berada diluar jam kerjanya, informasi mengenai gangguan pada jaringan dapat diketahui lebih awal. Hal ini bertujuan untuk mengantisipasi munculnya masalah lain yang jauh lebih besar pada jaringan.

CACTI adalah sebuah *tools* monitoring jaringan yang bekerja atas fasilitas SNMP (*simple network management protocol*) dan RRD Tools (*Round Robin Database Tool*) sehingga statistik kinerja jaringan dalam kurun waktu tertentu dapat dimonitor. CACTI juga merupakan sistem monitoring yang sudah dilengkapi fasilitas grafik untuk memunculkan statistik dari suatu jaringan dan fasilitas email untuk memberikan notifikasi masalah jaringan. Namun hingga tugas akhir ini dibuat, belum ada tambahan pada fitur CACTI berupa pesan singkat (*Short Messages Service*) untuk menotifikasi administrator tentang kerusakan yang terjadi pada jaringan. Oleh sebab itu, dalam tugas akhir ini akan diimplementasikan suatu sistem yang dapat memonitor kinerja jaringan menggunakan CACTI sekaligus memberikan notifikasi berupa *SMS (short message services)* kepada administrator jaringan agar penanganan masalah pada jaringan dapat dilakukan sedini mungkin.

Banyak hal yang menjadi pertimbangan dalam penggunaan dan pengembangan tools CACTI dalam tugas akhir ini. CACTI adalah *tools* monitoring yang bersifat *open source* yang berlisensi *GNU General Public Lisencc*, sehingga tidak akan memberatkan dari segi biaya lisensi. CACTI yang bersifat *open source* juga memungkinkan untuk dapat di-kustomisasi sesuai

kebutuhan dan digabungkan dengan beberapa tools monitoring lain yang sama-sama bersifat *open source*. *Patch* dan *plug-in* CACTI juga tersedia secara gratis di www.cacti.net sehingga tidak akan menyulitkan pengguna jika ingin mengupgradenya. Dibandingkan dengan pendahulunya seperti MRTG (*Multi Router Traffic Grapher*), tampilan CACTI jauh lebih menarik dan fitur monitoring yang ditawarkan juga lebih kompleks.

Masalah ataupun resiko yang dihadapi suatu jaringan memiliki tingkatan yang berbeda-beda. Adapun level skalabilitas dari ancaman menurut Roger S. Pressman (Pressman, 2005), dapat di definisikan dalam 4 kategori berikut :

1. *Catastrophics* (Bencana), pada level ini tingkat ancaman dapat dikategorikan sangat merusak. Dampak yang ditimbulkan dari tingkat ini dapat membuat sistem tidak berfungsi sama sekali.
2. *Critical* (Krisis), level ini dapat dikategorikan cukup merusak sistem, akan tetapi penggunaan kontrol yang diterapkan pada sistem telah dapat menahan kondisi kerusakan sehingga tidak menyebabkan kerusakan yang besar pada sistem
3. *Marginal* (kecil), Pada level ini kontrol keamanan mampu mendeteksi sumber ancaman yang menyerang sistem, walau tingkat kerusakan pada sistem masih terjadi akan tetapi masih dapat di perbaiki dan dikembalikan kepada kondisi semula
4. *Negligible* (dapat diabaikan), Pada level ini sumber ancaman tidak dapat mempengaruhi sistem, dimana kontrol atas sistem sangat mampu

mengantisipasi adanya kemungkinan ancaman yang dapat mengganggu sistem

Masing-masing kriteria resiko tersebut perlu penanganan yang berbeda. Masalah jaringan yang berdampak lebih besar pada sistem perlu penanganan sesegera mungkin dan perlu diprioritaskan. Oleh sebab itu, untuk menangani masalah tersebut perlu diterapkan metode antrian agar pesan peringatan (*alert*) yang disampaikan kepada administrator jaringan adalah pesan yang memiliki prioritas tertinggi. Metode antrian yang dipakai adalah *priority service*. Dengan demikian, konfigurasi dan pengaturan prioritas pesan terkirim dapat secara tepat dilakukan sesuai kondisi permasalahan jaringan pada waktu tertentu.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dibahas sebelumnya maka dapat diambil beberapa rumusan masalah :

1. Bagaimana menerapkan teknologi SMS (*short messages services*) pada CACTI sebagai fitur tambahan
2. Bagaimana metode antrian (*Priority Service*) dapat diterapkan pada proses pengiriman notifikasi (pesan peringatan) melalui fasilitas SMS

1.3 Batasan Masalah

Agar lebih terarah dan tidak menyimpang dari tujuan semula, maka penulis membuat batasan-batasan. Dalam tugas akhir ini, batasan masalah yang akan dibuat meliputi:

1. Sistem hanya melaporkan gangguan yang terjadi kepada administrator jaringan, dalam hal ini penanganan gangguan (*troubleshooting*) masih dilakukan secara langsung ke lokasi kejadian
2. SMS server yang akan digunakan adalah Now SMS Gateway
3. Sistem hanya difokuskan untuk memonitor jaringan dengan media transmisi kabel. Jaringan dengan media transmisi nirkabel tidak termasuk dalam cakupan bahasan
4. Sistem tidak dibuat untuk mengetahui jumlah pulsa pada modem dan kualitas sinyal layanan operator

1.4 Tujuan Penelitian

Penelitian yang dilakukan pada tugas akhir ini bertujuan untuk membangun sebuah sistem yang dapat memonitor aktifitas jaringan sekaligus memberikan laporan peringatan kepada administrator jaringan dalam bentuk SMS dengan menggunakan metode *priority service*.

1.5 Sistematika Pembahasan

Sistematika pembahasan yang akan digunakan dalam penulisan tugas akhir ini adalah:

Bab I Pendahuluan

Dalam bab ini penulis mengemukakan tentang gambaran keseluruhan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, metodologi penelitian serta sistematika pembahasan

Bab II Landasan Teori

Dalam bab ini, penulis mengemukakan analisa kinerja jaringan beserta parameternya, teknologi SMS, SNMP sebagai protokol yang bekerja untuk memonitor segala aktifitas jaringan serta *CACTI* sebagai tools monitoring jaringan yang merupakan implementasi dari SNMP dan teori dasar antrian

Bab III Metodologi Penelitian

Dalam bab ini menjelaskan mengenai cara yang dilakukan dalam menyelesaikan persoalan yang menjadi objek penelitian.

Bab IV Analisa dan Perancangan

Pada bab ini penulis menyajikan analisa kebutuhan penerapan *CACTI* sebagai sistem monitoring pada jaringan serta perancangan penambahan fitur pada *CACTI*.

Bab V Implementasi dan Pengujian

Bagian ini berisi proses implementasi serta skenario pengujian secara langsung pada jaringan yang akan membuktikan bagaimana proses notifikasi gangguan dengan menggunakan SMS tersebut bekerja.

Bab VI Kesimpulan dan Saran

Bagian ini memaparkan kesimpulan mengenai proses yang telah dilalui sebelumnya. Saran berisi perbaikan atas apa yang menjadi kekurangan dalam implementasi sehingga dapat menjadi acuan bagi pengembangan selanjutnya.

Statistik Wireless

- Sinyal yang didapat dan semua gangguan dari backbone nodes
- Jumlah dari stations yang terasosiasi.
- Mendeteksi jaringan dan kanal tetangga.
- Adanya pengiriman ulang yang terlalu banyak.
- Kecepatan data di radio, jika memakai automatic rate scaling

Statistik Switch

- Pemakaian Bandwidth per switch port
- Pemakaian Bandwidth per protokol

- Pemakaian Bandwidth per alamat MAC
- Trafik broadcast sebagai persentase dari total paket
- Kehilangan Packet dan rate error

Statistik Internet

- Internet bandwidth yang di pakai per host dan protocol
- Cache hits pada jaringan proxy
- 100 site yang paling sering diakses
- Permohonan DNS
- Jumlah dari email inbound / email spam / email bounce
- Besarnya antrian e-mail yang keluar
- Ketersediaan dari servis penting (jaringan web, jaringan email, etc.).
- Waktu Ping dan rate kehilangan paket ke ISP
- Status dari backup

Statistik kesehatan sistem

- Penggunaan memory
- Penggunaan swap file
- Process count / zombie process
- Sistem load
- Voltase dan load dari Uninterruptible Power Supply (UPS)
- Temperatur, kecepatan kipas, dan voltase sistem
- Status Disk SMART

- Status RAID array
- Jaringan komputer yang akan diambil sebagai tempat uji coba *CACTI* adalah jaringan LAN (*Local Area network*) pada Jurusan Teknik Informatika UIN Suska → diletakkan pada rencana uji coba di metodologi
- peralatan yang akan dimonitor adalah router 2600, hub, beberapa buah komputer dan laptop sebagai client, serta sebuah laptop sebagai server *CACTI* → dapat diletakkan pada perancangan ato mungkin pengujian sistem
- Parameter yang akan digunakan adalah kondisi *up* dan kondisi *down* dari suatu *host*, beban *traffic* masing-masing host, unjuk kerja (*utilization*) *host*, pemakaian memori, jumlah partisi dalam suatu *host* dan status dari masing masing interface pada sebuah router.

BAB II

LANDASAN TEORI

2.1 Analisa Kinerja Jaringan

Analisa kinerja jaringan didefinisikan sebagai suatu proses untuk menentukan hubungan antara 3 konsep utama, yaitu sumber daya (*resources*), penundaan (*delay*) dan daya-kerja (*throughput*). Obyektif analisa kinerja mencakup analisa sumber daya dan analisa daya kerja. Nilai keduanya ini kemudian digabung untuk dapat menentukan kinerja yang masih dapat ditangani oleh sistem.

Analisa kinerja pada jaringan komputer membicarakan sifat dasar dan karakteristik aliran data, yaitu efisiensi daya-kerja, penundaan dan parameter lainnya yang diukur untuk dapat mengetahui bagaimana suatu pesan diproses di jaringan dan dikirim lengkap sesuai fungsinya.

Analisa Kinerja jaringan komputer dapat didefinisikan sebagai penelitian kuantitatif yang terus menerus terhadap suatu jaringan komunikasi dalam urutan kerja yang tetap berada dalam fungsinya (Terplan, 1992) agar :

1. Dapat menyempurnakan level layanan pemeliharaan.
2. Dapat mengenali potensi kemacetan
3. Dapat mendukung pengendalian operasional jaringan, administrasi dan merencanakan kapasitas

Administrasi jaringan membantu langkah analisa kinerja dalam usaha mengevaluasi kemampuan layanan pada konfigurasi tertentu, selanjutnya akan

mendefinisikan indikator kinerja yang penting, merekomendasikan prosedur pelaporan kinerja dan menentukan antarmuka manajemen basis data.

2.1.1 Kategori dan Tujuan

Kategori :

1. Analisis kinerja dengan tujuan Optimalisasi Sistem dalam layanan yang cepat, tepat dan akurat.
2. Analisis kinerja dengan tujuan Optimalisasi Sistem dalam bidang keamanan sistem, data dan informasi, yang sering dikenal dengan istilah *Penetration Test* yaitu dengan cara melakukan penyelidikan terhadap sistem dari sudut pandang si penyerang. Tujuan utamanya adalah untuk mengidentifikasi temuan dan resikonya sebelum mencari suatu solusi.
3. Analisis Hybrid, analisis keseluruhan terhadap berbagai potensi sistem yang dapat ditingkatkan kinerjanya dengan tujuan evaluasi dan pengembangan sistem.

2.1.2 Parameter Kinerja Jaringan

Kriteria penting dari sudut pandang pemakai jaringan adalah keandalan, yaitu kriteria pengukuran seberapa mudah suatu sistem terkena gangguan, terjadi kegagalan atau beroperasi secara tidak benar. Keandalan adalah ukuran statistik kualitas komponen dengan menggunakan strategi pemeliharaan, kuantitas redudansi, perluasan jaringan secara geometris dan kecenderungan statis dalam merasakan sesuatu secara tidak langsung tentang bagaimana suatu paket ditransmisikan oleh sistem tersebut. Kinerja jaringan dapat diukur berdasarkan kriteria Terplan (1992) :

1. Kriteria level pemakai (user level), yaitu waktu respon dan keandalan
 - a. Waktu respon yaitu waktu tanggapan saat paket dipancarkan dengan benar.
 - b. Keandalan yaitu suatu keadaan yang dapat menentukan seberapa berfungsinya sistem pada suatu tugas pengiriman paket
2. Kriteria level jaringan (*network Level*), yaitu waktu respon rata-rata.
 Penentuan waktu respon rata-rata dilakukan dengan 2 langkah, yaitu :
 - a. Menentukan rata-rata penundaan satu jalur paket melewati jaringan dan antar mukanya sebagai suatu fungsi beban terhadap ukuran paket.
 - b. Menggunakan informasi dengan penundaan dan pemakaian link untuk menghitung waktu respon rata-rata pemakai
3. Kriteria kinerja khusus, yaitu daya kerja dan penundaan rata-rata.

2.1.3 SNMP Sebagai Indikator Kinerja Jaringan (*Utilization*)

Suatu jaringan komunikasi (termasuk jaringan komputer) tidak bisa dikelola bila indikator kinerjanya tidak dapat dipantau dan diukur dengan tepat. Salah satu syarat utama rancangan jaringan adalah menetapkan level layanan pemeliharaan untuk memuaskan pengguna sebagai basis analisis kinerja. Indikator kinerja haruslah dapat menunjukkan keadaan kinerja jaringan yang dipantau. Contoh suatu indikator kinerja adalah aplikasi SNMP (*Simple Network Management Protocol*), yang didalamnya terdapat MIB (*Management Information base*) yaitu struktur database variabel elemen jaringan yang dikelola yang dikelompokkan berdasarkan parameter layanan dan parameter efisiensi.

2.1.3.1 Parameter Layanan

Merupakan suatu ukuran yang berorientasi pada pelayanan jaringan dan lebih mempertimbangkan minat pemakai. Parameter ini mengontrol dan merencanakan ketersediaan jaringan yang terdiri atas :

1. Parameter Ketersediaan

Availabilitas fungsi jaringan adalah presentasi waktu pengguna terhadap akses total layanan jaringan yang tersedia baginya, yang amat tergantung pada keandalan komponen secara teknis. Parameter ini tidak diukur secara langsung, tapi dihitung menggunakan data indikator kinerja (Terplan, 1992) yang terdiri dari:

- a. *Overall network availability*, ketersediaan jaringan secara menyeluruh, diambil dengan mengumpulkan data dari beberapa simpul jaringan yang penting.
- b. *Line availability*, ketersediaan jalur jaringan, mengukur ketersediaan simpul menerima dan meneruskan paket/frame informasi dari simpul ke simpul dan menginformasikan paket-paket yang diabaikan karena keterbatasan sumber daya (*In/OutDiscard*) selama pemantauan (*SysUpTime*).
- c. *Customer level availability*, ketersediaan pada level user, diukur dari data pemakaian terminal atau simpul terminal.

2. Parameter waktu respon

Indikator waktu respon (Terplan, 1992) terdiri dari :

- a. *Network delay*, penundaan pada jaringan.

- b. *Host delay*, penundaan pada host dan simpul jaringan, menetapkan lama penundaan waktu dalam komputer pusat untuk suatu paket sampai ke komputer tujuan.
- c. Waktu respon rata-rata
- d. Waktu respon maksimal, menetapkan harga maksimum lamanya suatu paket/datagram diizinkan dalam suatu jaringan.
- e. Waktu respon minimal
- f. Alternatif pada level user : daftar pertanyaan

Besarnya nilai waktu respon dapat dipantau dengan cara memanfaatkan aplikasi *ping* yang mengirimkan datagram *echo-request* dari protokol ICMP untuk mendapatkan datagram *echo-respon* dari suatu simpul jaringan.

3. Parameter keandalan

Indikator keandalan (reliabilitas) terdiri dari :

- a. Jumlah *failure* pada elemen jaringan, memberitahukan suatu gateway tertutup untuk dilewati
- b. Daftar tindakan pada kesalahan yang paling sering terjadi.
- c. Jumlah pesan-pesan yang hilang
- d. Jumlah pesan yang harus diduplikasi
- e. Jumlah pesan yang tiba, tetapi tidak disampaikan
- f. Jumlah pesan yang menyatakan kiriman telah diterima
- g. Jumlah transmisi ulang
- h. Jumlah *time out*, waktu yang tidak terpakai karena *idle*
- i. Jumlah transmisi yang tidak lengkap.

2.1.3.2 Parameter Efisiensi

Merupakan ukuran kinerja yang mementingkan bagaimana informasi bekerja secara efisien dan ukuran daya kerjanya. Daya kerja (*throughput*) dalam bit per detik, didefinisikan sebagai rata-rata lewatnya bit data pada simpul jaringan tertentu per satuan waktu. Pada jaringan kondisi tetap, kecepatan masuk dan keluarnya paket adalah sama, maka daya kerja adalah harga rata-rata bit per detik tiap memasuki atau meninggalkan jaringan. Indikator parameter daya kerja menurut Terplan(1992) terdiri dari :

1. *Transmit*, terdiri dari : jumlah transaksi, jumlah paket, jumlah pesan, jumlah karakter, pesan terpanjang dan rata-rata panjang pesan yang dipancarkan.
2. *Receive*, terdiri dari : jumlah transaksi, jumlah pesan, jumlah paket, jumlah karakter pesan terpanjang dan rata-rata panjang pesan yang diterima.
3. *Polling*, terdiri dari : jumlah pool positif, jumlah pool negatif dan jumlah pool penundaan
4. *Utilization*, terdiri dari : utilisasi pengendalian komunikasi (pemanfaatan protokol IP, ICMP, TCP, SNMP), pengendalian *cluster* (pada protokol IP) dan utilisasi peralatan terminal
5. *Link idle*, memantau hubungan yang tidak terjadi antara simpul jaringan pada saat tertentu.
6. *Link utilization*, memantau hubungan yang terjadi antara simpul jaringan pada saat tertentu.

7. *Contention*, memantau terjadinya ‘tabrakan’ (*collision*) pada fungsi perangkat (perangkat keras dan lunak) jaringan dan elemen jaringan.

2.2 Standar Keamanan Jaringan dan Contoh Permasalahan Jaringan

Jaringan komputer dan sistem yang terdapat didalamnya selalu terdapat kelemahan dan kekurangan. Hal yang lazim dilakukan adalah menemukan kekurangan tersebut untuk kemudian memperbaikinya. Oleh sebab itu, CACTI diberi tambahan fitur baru berbasis sms agar kekurangan yang ada dapat tertutupi.

Sebelum membicarakan mengenai masalah yang kerap terjadi di jaringan, ada baiknya kebutuhan minimal untuk keamanan sebuah jaringan komputer dipaparkan terlebih dahulu. Hal ini perlu dibahas sebab masalah jaringan akan selalu membayangi seorang administrator apabila standar minimal keamanan yang harus dimiliki oleh jaringan tidak dipenuhi. Standar keamanan jaringan dimaksudkan mengenali komponen-komponen yang harus diberikan perlindungan agar tercapai suatu lingkungan jaringan yang aman dengan kebutuhan minimum sebagai berikut (Sysneta, 2010):

1. Semua titik-2 yang bisa diakses secara fisik dan juga perangkat jaringan (routers, server dan LAN Switches) haruslah aman secara fisik. Jangan sampai *infrastructure* vital (misal server room) bisa diakses oleh sembarang orang, bahkan bila perlu disamarkan tanpa ada yang tahu fungsinya.
2. Operating system dan firmware piranti haruslah diperkuat (*dipatched / diupdate*) untuk mencegah titik-titik lemah keamanan (*security hole*)

3. Piranti-2 jaringan seperti switches dan router haruslah mempunyai password yang sangat kuat, password yang tidak umum dan tidak gampang ditebak.
4. Akses remote kepada piranti jaringan (Telnet) haruslah di control dengan membatasi aksesnya menggunakan system filter IP address kepada remote device yang memang diberikan akses saja dan hanya oleh personal IT support saja.
5. Piranti jaringan haruslah mempunyai “*Message of the Day (MOTD)*” atau banner login yang mendefinisikan Warning pesan Legal setiap kali diakses, dengan pesan larangan kepada semua user yang tidak terotorisasi jika mencoba untuk mengakses piranti jaringan tersebut.
6. Session time-out pada console dan telnet haruslah di setting dan dibatasi tidak boleh lebih dari 10 menit saat idle kepada semua piranti jaringan. Hal ini untuk menjaga pelanggaran keamanan jika terminal tersebut ditinggal dalam keadaan masih logon.
7. Password dan nama community SNMP haruslah paling sedikit 8 karakter dan haruslah terdiri dari alphanumeric password. Password haruslah tidak gampang ditebak.
8. Management services seperti SNMP haruslah didisable jika tidak dipakai
9. Semua komunikasi public (internet dan wireless) haruslah di enkripsi. Enkripsi haruslah secara regular diganti dengan cara yang aman untuk menjaga pengupingan dan serangan manipulasi data.

10. Pertahanan perimeter haruslah ditekankan pada segenap titik jaringan yang menghadap ke public termasuk internet. Hal ini bisa dilakukan dengan menggunakan paket filtering (extended access-list). Untuk koneksi ke internet sebuah firewall dengan konfigurasi policy yang sangat kuat haruslah diterapkan. Gunakan policy yang sangat ketat untuk inbound traffic dari internet dengan extended access-list pada semua parameter router. Access-list haruslah simple dan sangat efektif dalam mengontrol traffic yang tidak diinginkan dan memberikan keamanan kuat kepada asset penting.

Selain itu, seorang pakar teknologi jaringan David Icove mengklasifikasikan tingkat keamanan yang harus diperhatikan meliputi (Yodi, 2010):

1. Fisik / *Physical Security*
2. Manusia / *Personel Security*
3. Data, media , teknik dan komunikasi
4. Kebijakan dan prosedur

Penjelasan masing-masing tingkat keamanan tersebut terhadap keamanan jaringan adalah sebagai berikut : untuk tingkat keamanan secara fisik adalah memastikan semua komponen fisik jaringan terpasang secara benar. Keamanan fisik lebih dipandang pada sisi hardware dari jaringan komputer serta peralatan pendukungnya, seperti AP (Access Point), Kabel LAN (Local Area Network), *cable tray*, Chasing CPU, UPS, AC untuk ruangan server dan lain sebagainya.

Keamanan terhadap personel (*personel security*) yang menggunakan jaringan komputer perlu diperhatikan. Sebagai contoh kasus Kevin Mitnick (Hacker Legendaris), dimana dia mampu menjebol sistem keamanan perusahaan dengan cara berpura-pura menjadi pegawai service komputer. Hal yang mungkin terjadi adalah sistem keamanan jaringan komputer rusak gara-gara orang asing yang masuk ataupun personel yang bekerja dalam jaringan itu sendiri. Bila terkait dengan orang asing, keamanan bisa dibentuk dengan membuat sistem ID-CARD, penempatan petugas keamanan ataupun penerapan level personel. Bagaimana bila orang dalam? Sangat sulit membentuk standar keamanan personel karena ini berkaitan dengan etika dan moral dari personel itu sendiri. Satu-satunya harapan adalah HRD mampu menyeleksi pegawai yang jujur dan bisa dipercaya dalam bekerja.

Keamanan pada bidang data, media, teknik dan komunikasi cenderung mendapatkan perhatian yang lebih daripada yang lain. Keamanan pada sisi ini menitikberatkan pada aspek software. Data pada jaringan tentu harus diamankan dari berbagai pihak yang tidak memiliki izin khusus. Dalam jaringan komputer dapat ditentukan medianya untuk berkomunikasi menggunakan media dan teknik tertentu. Contoh kasusnya, komunikasi transfer file dilakukan dengan sistem sharing. Ada pemberian izin kepada komputer tertentu yang bisa mengakses data-data penting. Dalam jaringan tersebut, menggunakan media sharing file system (seperti NFS (*Network File System*) dalam pertukaran data. Secara teknik, tiap- tiap komputer harus mengetahui alamat komputer lain bila hendak melakukan sharing. Dalam gambaran umum tersebut, keamanan ditingkatkan dengan cara

menggunakan password dalam pengaturan hak pengaksesan data. Selain itu, komputer lain tidak boleh menggunakan media lain selain sistem file sharing dalam berkomunikasi.

Kebijakan (*policy*) serta prosedur dalam jaringan komputer harus ditentukan secara tegas guna membangun sistem keamanan yang kuat. Penggolongan beberapa pengguna jaringan komputer terhadap kepentingannya haruslah diperhatikan. Aplikasinya, bila pada suatu jaringan komputer perusahaan, terdapat 3 bidang kerja yaitu keuangan, customer service dan produksi. Pengaturan kebijakan dan prosedur diterapkan berdasarkan kepentingan bidang kerja masing-masing. Contohnya, perusahaan tersebut mendapatkan koneksi internet. Perlu dilihat bahwa kepentingan divisi keuangan yang tidak membutuhkan internet dalam operasionalnya. Sedangkan divisi *customer service* dan produksi membutuhkan akses internet dalam operasionalnya. Maka pengaturan kebijakan disini adalah koneksi internet cuma diberikan pada jaringan komputer divisi customer service dan produksi sedangkan divisi keuangan tidak diberikan akses internet. Namun secara total, jaringan komputer divisi keuangan, divisi customer service serta divisi produksi saling terhubung satu dengan yang lain.

Penjelasan panjang mengenai keamanan jaringan diatas bukan sekedar wacana, akan tetapi terlebih dahulu memang wajib diterapkan pada jaringan komputer untuk meminimalisir resiko yang akan terjadi. Bersamaan dengan hal itu, penggunaan system monitoring juga sangat perlu diterapkan guna memberikan jaminan ketersediaan akses ke jaringan karena tujuan utama sebuah

sistem monitoring adalah memastikan bahwa jaringan komputer selalu *available* (tersedia). Jika hal tersebut tidak dimungkinkan, maka tujuan utama selanjutnya adalah memastikan bahwa informasi ketidaksediaan jaringan tersebut dapat diperoleh dengan cepat.

Ketidaksediaan dalam jaringan sering dikaitkan dengan berbagai masalah yang terjadi di jaringan. Masalah yang terdapat pada jaringan dapat dikelompokkan dalam dua kategori; yakni masalah jaringan yang berhubungan dengan konektifitas dan masalah yang berkaitan dengan kinerja jaringan (Ekklesya, 2009).

Masalah konektifitas terjadi ketika suatu *End Station* (seperti komputer, hub/switch, router) tidak dapat berkomunikasi satu sama lain baik di lingkungan jaringan LAN (Lokal Area Network) maupun WAN (Wide Area Network). Masalah konektivitas meliputi *Lose of Connectivity* dan *Intermittent Connectivity*

a. Kehilangan Konektifitas (*Lose Of Connectivity*)

Lose of Connectivity (LoC) adalah suatu kondisi yang terjadi dimana para pengguna layanan jaringan tidak dapat mengakses jaringan sama sekali. Penyebab terjadinya masalah ini bisa bermacam-macam, akan tetapi secara umum masalah ini hampir dapat dipastikan karena terjadinya kesalahan dan kerusakan pada peralatan fisik di jaringan. Sebagai contoh; kabel yang rusak, peralatan pada server farm misalkan router yang tiba-tiba mati karena terlalu panas, kesalahan konfigurasi routing pada router sehingga menyebabkan koneksi gagal dengan status *ip acquiring*, dan sebagainya.

b. Konektivitas Terputus – Putus Atau Tidak Stabil (*Intermittent Connectivity*)

Kondisi ini terjadi apabila para pengguna memiliki akses kesumber daya jaringan beberapa kali tetapi mereka kadang kala masih menghadapi koneksi jaringan yang “mati” (*Periods Of Downtime*). Masalah konektivitas yang terputus – putus dapat mengindikasikan bahwa jaringan berada pada ambang kerusakan yang lebih parah. Masalah ini pada beberapa kasus berkemungkinan dapat disebabkan oleh permasalahan fisik yang tidak baik (misalkan voltase yang tidak stabil sehingga transfer data terputus-putus), sementara pada beberapa kasus lainnya disebabkan oleh masalah kinerja yang akan dibahas selanjutnya.

Masalah kinerja jaringan merupakan masalah yang timbul pada jaringan ketika ia tidak dapat beroperasi secara efektif sesuai dengan sumber daya dan beban kerja yang ada. Sebagai contoh, waktu respon jaringan tidak stabil seperti biasanya, dan para pengguna banyak yang mengeluh bahwa jaringan melayani pekerjaan mereka lebih lama. Beberapa masalah kinerja yang bersifat sewaktu – waktu muncul seperti duplikasi alamat dan laju utilisasi jaringan yang selalu konsisten tinggi dapat saja terjadi. Contoh lain yang dapat mengganggu kinerja jaringan adalah terjadinya down pada suatu titik di jaringan karena lalu lintas paket pada suatu waktu melebihi kapasitas bandwidth, kapasitas log server yang terlalu penuh, kapasitas hardware dan memori yang sudah tidak lagi memadai karena meningkatnya aktifitas jaringan, transfer data yang tiba-tiba melambat yang bisa saja dikarenakan penambahan jumlah user yang tidak terotorisasi.

Masalah kinerja jaringan yang buruk dan tidak segera diperbaiki akan menimbulkan masalah lain yang berdampak jauh lebih besar terutama pada keberlangsungan bisnis yang ditangani oleh jaringan. Oleh sebab itu untuk menangani masalah inipun diperlukan cara dan prosedur yang tepat.

2.3 Manajemen Jaringan

Dengan berkembangnya jaringan TCP/IP yang sangat pesat, maka diperlukan juga suatu manajemen untuk mengatur jaringan. *Internet Architecture Board* (IAB) merekomendasikan RFC 1052 yang berisikan tentang :

2 *Simple Network Management Protocol* (SNMP)

3 *ISO Common Management Information Service / Common Management Information Protocol* (CMIS / CMIP)

IAB menyarankan untuk menggunakan SNMP

2.3.1 Simple network Management Protocol (SNMP)

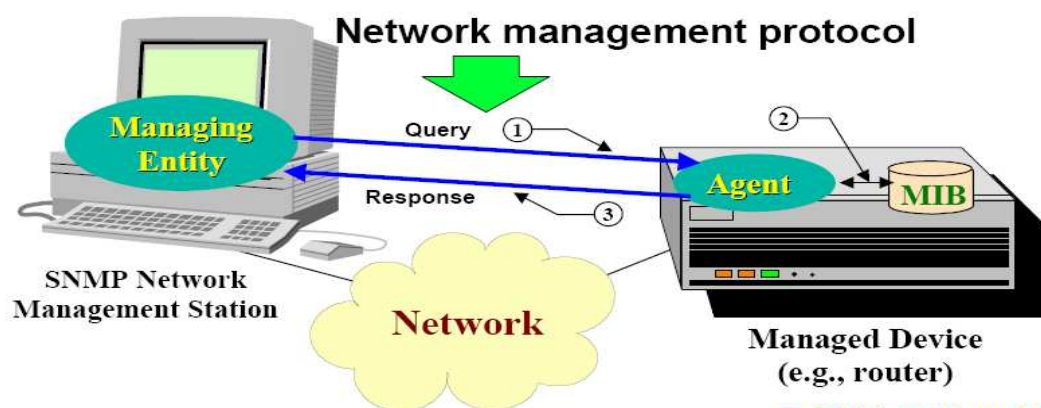
SNMP (protokol manajemen jaringan yang bersifat simpel) merupakan salah protokol resmi dari Internet Protocol suite yang dibuat oleh *Internet Engineering Task Force* (IETF). SNMP merupakan contoh dari layer 7 aplikasi yang digunakan oleh *network management sistem* untuk memonitor perangkat jaringan sehingga dapat memberikan informasi yang dibutuhkan bagi pengelolaanya.

2.3.2 Konsep SNMP

SNMP digunakan untuk me-manage perangkat yang berada di dalam internet menggunakan protokol TCP/IP. SNMP menyediakan sekumpulan operasi dasar untuk memantau (monitoring) dan me-maintain internet. SNMP

menggunakan konsep manager dan agent. Manager (biasanya berupa suatu host) mengendalikan dan memantau sekumpulan agent.

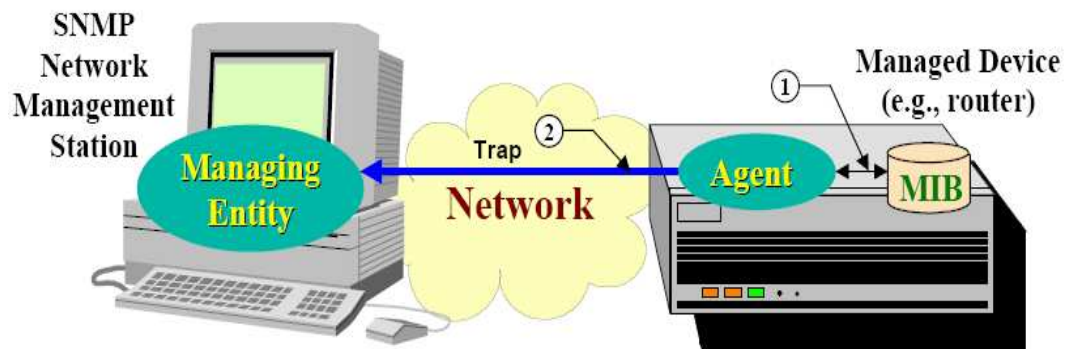
Management station (disebut manajer) merupakan suatu host yang menjalankan program *SNMP client*. *Managed station* (disebut agent) adalah router atau host yang menjalankan program *SNMP server*. Manajemen jaringan diperoleh melalui interaksi antara manager dengan agent



Gambar 2.1 SNMP Manager meminta Informasi pada SNMP Agent

Gambar 2.1 menjelaskan interaksi yang terjadi antara *management station* (manajer) dengan *agent*. Untuk mendapatkan informasi yang terdapat pada database agent (MIBs), manager akan mengirimkan permintaan berupa *query* pada agent. Agent memiliki dan menyimpan informasi *performance* di dalam suatu *database* yang disebut MIB (Management Informatin Based). Agent akan berinteraksi dengan MIB dan memproses query.

Setelah query diproses, agent akan mengirimkan respon berupa trap. Trap adalah pesan yang dikirimkan dari agent ke manager sebagai laporan dari suatu event. Gambar 2.2 dibawah ini mendeskripsikan tentang proses pengiriman trap.



Gambar 2.2 SNMP Agent Memberikan Response Berupa Trap Pada SNMP
Manager

Manager dapat mempunyai akses terhadap nilai (value) yang terdapat di dalam database tersebut. Misalnya sebuah router menyimpan informasi variabel jumlah paket yang diterima dan jumlah paket yang di-forward; manager dapat mengambil dua informasi tersebut lalu membandingkannya untuk mengambil keputusan apakah router tersebut sedang berada di dalam kondisi kongesti atau tidak

Manager dapat pula menyuruh router (host) untuk melakukan aksi tertentu. Agent dapat pula berkontribusi terhadap proses manajemen. Program server yang berjalan di agent dapat mengecek kondisi router dan bila ditemukan gejala yang tidak biasa, maka agent dapat mengirimkan pesan peringatan (*warning message*) yang disebut *trap* ke manager

Dengan kata lain, proses manajemen SNMP menggunakan tiga ide dasar:

1. Suatu manager mengecek suatu agent dengan cara meminta informasi kelakuan agent
2. Suatu manager dapat memaksa agent untuk melaksanakan tugas tertentu dengan me-reset nilai (value) di dalam database agent

3. Agent berkontribusi terhadap proses manajemen dengan memperingatkan manager bila terdapat situasi yang tidak biasa.

2.3.3 Management Information Base (MIBs)

MIB merupakan database yang digunakan untuk manajemen perangkat pada jaringan. Database tersebut berisikan objek entiti dari perangkat jaringan (seperti router atau switch). Objek pada MIB didefinisikan menggunakan Abstract Syntax Notation One (ASN 1), dan diberi nama “Structure of Management Information Version 2 (SMIv2). Software yang digunakan untuk parsing disebut MIB compiler.

RFC yang membahas antara lain RFC1155 – Structure and identification of Management Information for TCP/IP base internets, RFC1213 – Management Information Base for Network Management of TCP/IP-based internets, dan RFC 1157 – A Simple Network Management Protocol.

SNMP, komunikasi yang terjadi antara management station (contoh: console) dengan management object (seperti router, gateway dan switch), menggunakan MIB. Component yang berkerja untuk mengambil data disebut SNMP agent, merupakan software yang dapat berkomunikasi dengan SNMP Manager.

2.3.4 Arsitektur SNMP

Framework dari SNMP terdiri dari :

1. Master Agent

Master agent merupakan perangkat lunak yang berjalan pada perangkat yang mendukung SNMP, dimana bertujuan untuk merespon permintaan dari

SNMP dari *management station*. Master agent kemudian meneruskan kepada *subagent* untuk memberikan informasi tentang manajemen dengan fungsi tertentu.

2. *Subagent*

Subagent merupakan perangkat lunak yang berjalan pada perangkat yang mendukung SNMP dan mengimplementasikan MIB. *Subagent* memiliki kemampuan:

- a. Mengumpulkan informasi dari objek yang *dimanage*
- b. Mengkonfigurasi informasi dari objek yang *dimanage*
- c. Merespon terhadap permintaan manajer
- d. Membangkitkan alarm atau trap

3. *Management Station*

Management station merupakan client dan melakukan permintaan dan mendapatkan trap dari SNMP server.

2.3.5 Protokol SNMP

PDU dari SNMP (versi 1) antara lain :

1. GET REQUEST – digunakan untuk mendapatkan informasi manajemen
2. GETNEXT REQUEST – digunakan secara iteratif untuk mendapatkan sekuen dari informasi manajemen
3. GET RESPONSE
4. SET – digunakan untuk melakukan perubahan terhadap subsistem
5. TRAP – digunakan untuk melakukan pelaporan terhadap subsistem manajemen

Untuk versi berikutnya ditambahkan PDU :

1. GETBULK REQUEST – iterasi yang lebih cepat untuk mendapatkan informasi
2. INFORM – acknowledge terhadap TRAP

SNMP menggunakan UDP pada port 161 untuk agent dan 162 untuk manager. Manager mengirimkan permintaan terhadap agent pada port 161 dan diterima oleh manager pada port 162.

2.3.6 Perkembangan SNMP

2.3.6.1 SNMP Version 1

RFC untuk SNMP, dikenal dengan nama Simple Network Management Protocol

version 1, pada tahun 1988 :

1. RFC 1065 – *Structure and identification of management information for TCP/IP-based internets*
2. RFC 1066 – *Management information base for network management of TCP/IP-based internets*
3. RFC 1067 – *A Simple Network Management Protocol*

Kemudian menjadi kadaluwarsa dengan digantikan dengan :

1. RFC 1155 – *Structure and identification of management information for TCP/IP-based internets*
2. RFC 1156 – *Management information base for network management of TCP/IP-based internets*
3. RFC 1167 – *A Simple Network Management Protocol*

Versi 1 memiliki kelemahan pada sistem autentifikasi karena mengirimkan password secara plain text.

2.3.6.2 SNMP Version 2

Versi 2 ini banyak yang tidak menggunakan dikarenakan ketidakcocokan framework. *Simple Network Management Protocol* version 2 (RFC 1441 – RFC 1452) dan juga dikenal sebagai SNMP v2. Diperkenalkan GETBULK sebagai alternatif dari GETNEXT. Dikenalkan juga *Community-Based Simple Network Management Protocol* version 2 atau yang disebut SNMP v2c sebagai pengganti sistem autentikasi *User-Based Simple Network Management Protocol* version 2, atau SNMP v2u yang digunakan untuk memperbaiki keamanan dari SNMP v1.

2.3.6.3 SNMP Version 3

Versi ini didefinisikan pada RFC 3411 – RFC 3418 yaitu *Simple Network Management Protocol* version 3, dikeluarkan pada tahun 2004. Pada prakteknya SNMP bisa menggunakan versi SNMPv1, SNMPv2c, atau SNMPv3. Dijabarkan pada RFC 3584 – Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework.

2.3.6.4 Contoh Penggunaan SNMP

Beberapa contoh penggunaan SNMP:

1. Memonitoring waktu penggunaan suatu perangkat (*sysUpTimeInstance*)
2. Inventory dari versi sistem operasi (*sysDescr*)
3. Mengkoleksi informasi suatu interface (*ifName*, *ifDescr*, *ifSpeed*, *ifType*, *ifPhysAddr*). Mengukur throughput interface dari jaringan (*ifInOctets*, *ifOutOctets*, *ifInErrors*, *ifOutErrors*), yakni jumlah total byte

yang diterima dan jumlah total byte yang dikirim. , ifInErrors mendefinisikan jumlah paket diterima yang dibuang karena rusak, ifOutErrors mendefinisikan jumlah paket dikirim yang dibuang karena rusak

4. Menarik informasi cache dari ARP (ipNetToMedia)

2.3.7 Implementasi SNMP

2.3.7.1 SNMP walk

```
snmpwalk -c public punch system
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3-M), Version 12.2(15)T5, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 12-Jun-03 15:49 by eaarn
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.107
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (835747999) 96 days, 17:31:19.99
SNMPv2-MIB::sysContact.0 = STRING: wikiuser
SNMPv2-MIB::sysName.0 = STRING: punch
SNMPv2-MIB::sysLocation.0 = STRING: test
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

Gambar 2.3 Implementasi Snmp walk

2.3.7.2 Router Graphing Software

Banyak informasi yang bisa ditampilkan, misal performance, load dan error rate dari suatu jaringan seperti router atau switch. Kemudian dengan fungsi khusus, informasi yang didapat diolah menjadi dalam bentuk grafik. Contoh aplikasinya adalah Multi Router Traffic Grapher dan CACTI

2.4 CACTI

CACTI merupakan software graphing /perekam dalam bentuk grafis untuk melihat seberapa besar traffic yang terjadi, baik inbound maupun outbond dalam suatu jaringan client-server. CACTI adalah hasil pengembangan paling lengkap dari RRD tool- yang menyimpan semua informasi yang diperlukan untuk

membangun grafik dan menyimpannya dalam basis data Mysql.CACTI dibangun menggunakan skrip PHP dan selain bisa digunakan untuk membangun suatu grafik, Data source (sumber data) dan arsip-arsip Round Robin dalam basis data, CACTI mampu menangani pengumpulan data itu sendiri. CACTI berjalan dengan fasilitas SNMP sehingga semua fungsi yang dimiliki oleh SNMP telah diadopsi oleh CACTI termasuk fasilitas keamanan karena CACTI mendukung SNMP versi 1 dan versi 2. Sehingga dengan CACTI Network administrator akan lebih mudah memanage performa/ unjuk kerja jaringan, menemukan dan menyelesaikan masalah jaringan dan merencanakan untuk perkembangan jaringan selanjutnya

2.4.1 Data Source

Untuk menghandel pengumpulan data , dapat dibuat eksternal script atau command yang akan diperlukan untuk di pilih, CACTI kemudian menyimpan nya kedalam database. Data Sources dapat juga di buat, yang berkoresponden dengan data sebenarnya dalam grafik. Sebagai contoh jika ingin membuat grafik ketika ping ke suatu host, harus dibuat data sources dengan memanfaatkan skrip yang meng-ping suatu host yang menghasilkan nilai dalam milliseconds. Setelah itu dapat didefinisikan informasi tambahan yang dibutuhkan oleh data input. Seperti *host* yang akan di ping dalam hal ini. Setelah data source di buat, lalu akan di maintain setiap 5 menit secara otomatis.

2.4.2 Graph (Grafik dalam CACTI)

Pengumpulan data pada CACTI untuk ditampilkan dalam grafik dapat dilakukan secara *real time*. Dan setiap data yang dikumpulkan akan dapat

disimpan dalam basis data untuk kemudian dilakukan pengukuran kembali sesuai waktu yang diinginkan, misalkan setiap lima menit sekali grafik utilitas suatu perangkat jaringan akan ditampilkan.

Satu atau lebih data yang telah ditetapkan, grafik RRD tool akan dapat digunakan untuk membangun data tersebut. CACTI menyediakan fasilitas untuk manage grafik tersebut berdasarkan fungsi dan tipe yang berbeda. Pemilihan warna serta fungsi tulisan juga ditambahkan agar proses monitoring berjalan lebih mudah.

2.4.3 *User Management* (Manajemen Pengguna)

Berhubung CACTI memiliki fungsi yang sangat banyak terhadap jaringan, maka manajemen berbasis user sengaja ditambahkan untuk menjaga otoritas terhadap user yang memiliki hak akses. Hal ini akan mengakibatkan seseorang yang memiliki otoritas mampu merubah parameter dari grafik sementara pengguna lain hanya mampu melihat tampilan dari grafik saja.

2.4.4 *Templating*

CACTI dapat diskalakan menjadi jumlah besar *data sources* dan dituangkan dalam bentuk grafik dengan penggunaan *template*. Hal ini akan memungkinkan pembuatan grafik tunggal ataupun *data source template* yang tentu saja akan menegaskan grafik dan data source yang tergabung didalamnya. *Host template* dalam CACTI mampu mengukur kemampuan / kapabilitas dari suatu host sehingga CACTI juga mampu membuat polling ketika penambahan host baru.

Kebutuhan awal yang harus dipenuhi oleh sistem sebelum instalasi CACTI adalah sebagai berikut:

1. Web Server (Apache)
2. PHP (PHP5)
3. Database mySQL (mysql 5)
4. Net-SNMP
5. RRDTool

RRD (Round Robin Database), merupakan suatu sistem yang menyimpan dan menampilkan data time-series seperti: network bandwidth, temperatur CPU, utilisasi load average. Dengan memanfaatkan RRDTool data-data tersebut dapat dilihat dalam jangka waktu tertentu, dengan menggunakan skrip yang simpel (php) agar data-data yang disimpan tadi dapat divisualisasikan lebih *user friendly*, dan dalam hal ini pengguna tidak akan menemui kesulitan memvisualisasikannya karena CACTI sudah membundelnya dalam satu paket.

Cukup banyak aplikasi-aplikasi Open Source NMS yang menggunakan RRD Tool sebagai dasar dalam membuat grafik hasil pengkoleksian data dari perangkat jaringan. Konsepnya dari RRD tool sangat sederhana. Analoginya adalah dalam sebuah lingkaran, di sepanjang garis pinggir lingkaran itulah data akan disimpan, dalam sebuah titik yang dipilih. Kemudian dari titik itu ditarik garis ke arah titik pusat, sehingga menjadi 'pointer' terhadap titik yang ada di pinggir. Penulisan dan pembacaan data menggunakan pointer tersebut. Dan karena berbentuk lingkaran maka dapat ditulis berulang-ulang tanpa batas waktu. Tentu saja akan ada waktunya data yang pertama kali ditulis akan tertimpa data terbaru.

Tetapi keuntungannya adalah tidak perlu khawatir *database* akan bertambah besar, dan itu berarti proses *maintenance* database tidak akan menyulitkan.

Beberapa aktifitas monitoring yang dapat dilaporkan oleh CACTI:

1. CACTI dapat digunakan untuk menginventori semua peralatan/ device yang connect ke network, meski begitu CACTI yang sudah ada harus dikustomisasi (patch dan programnya harus diatur sedemikian rupa sesuai kebutuhan)
2. Pemantauan Link dan traffic serta aktifitas pada jaringan
3. Mendapatkan info network interface.
4. Kapasitas partisi hardisk
5. Beban prosesor
6. Penggunaan memori
7. *Space of disk in server*, ruang penyimpanan dalam server
8. Temperatur Ruang Server
9. *CPU utilization* (kinerja CPU)

Hal lain yang mampu dilakukan oleh CACTI:

1. CACTI juga bisa digunakan untuk membuat trap squid proses kedalam grafik. Hal tersebut antara lain:
 - a. *Squid Available File Descriptor*
 - b. *Squid Cache Hit Rate*
 - c. *Squid Client Request Rate*
 - d. *Squid CPU Usage*

2. Pada sebuah mikrotik bridge, mikrotik traffic flow dapat diukur menggunakan CACTI :
 - a. untuk menampilkan trafic ip yang melewati mikrotik bridge
 - b. users bisa memonitor trafiknya sendiri

Berikut merupakan contoh penerapan penggunaan CACTI pada peralatan jaringan :

1. Jumlah dari sukses tidaknya percobaan pengalokasian Internal router buffer sebagai tempat penyimpanan informasi. Nilainya akan memberitahukan pada admin jika router sedang dalam bahaya akan hilangnya paket yang bisa disebabkan oleh kurangnya ketersediaan space antrian
2. Rata-rata dari penggunaan CPU setiap periode 5menit. Nilai ini akan memberikan informasi mengenai router, apakah *overused*, *underused* ataupun *corectly used*.
3. Temperatur udara yang masuk dan keluar dari router. ini akan memberikan admin info tentang situasi lingkungan router. suhu masuk terlalu tinggi kalo router diinstall dalam ruangan yang kurang ventilasi. Kalo suhu keluarnya tinggi, jika satu atau lebih ventilasi udara router tertutup.
4. Voltase yang ada dalam bermacam barisan listrik di router. nilai ini akan memberikan info ke admin tentang status kelistrikan router. Khususnya voltase +5 dan +12 ke power suply nya router bisa diketahui. Nilai abnormal tentunya akan mengindikasikan kesalahan pada power supply.

2.5 SMS (*Short Message Service*)

2.5.1 Pengertian SMS

Short Message Service (SMS) adalah kemampuan untuk mengirim dan menerima pesan yang terbatas besarnya (pesan singkat) antar *handphone*/ telepon selular yang berupa data dalam bentuk *string* atau teks dan data *binary*. Teks dapat terdiri dari kombinasi kata-kata, nomor-nomor, atau penggabungan huruf dan angka. Setiap SMS dibatasi hanya sampai 160 karakter saja, dengan menggunakan huruf latin, sedangkan untuk karakter non latin seperti karakter Arab atau *Chinese*, SMS dibatasi hanya sampai 70 karakter saja. *Output* pada MS (*Mobile Station*) dari data yang diterima dalam bentuk teks adalah teks juga, sedangkan *output* dari data *binary* bisa berupa teks, gambar maupun suara (*mail box*).

SMS termasuk salah satu dari GSM data *services* yang disediakan oleh PLMN (*Public Land Mobile Network*). Contoh GSM data *services* yang lain adalah *fax* dan data *transfer*. GSM data *services* hanya dapat digunakan jika sebuah PLMN menyediakan fasilitas tersebut. SMS pertama dikirim pada bulan Desember 1992, dari sebuah PC (*Personal Computer*) ke sebuah *handphone* pada Vodafone GSM *network* di Inggris.

2.5.2 Fasilitas Dasar SMS

Ada dua macam fasilitas dasar pada SMS, yaitu:

1. SM MT (*Short Message Mobile Terminated*)
2. SM MO (*Short Message Mobile Originated*)

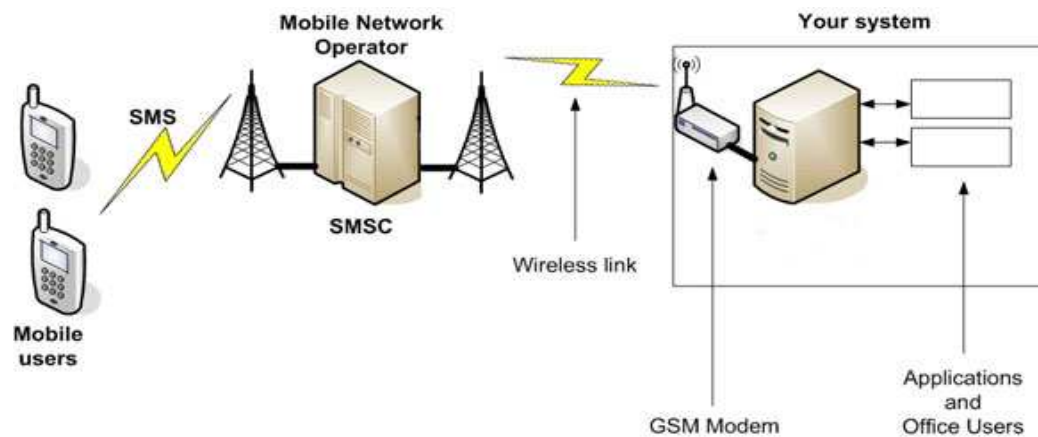
SM MT merupakan kemampuan untuk mentransfer sebuah pesan singkat yang dikirim dari SC ke salah satu MS, dan menyediakan informasi tentang pengiriman pesan tersebut apakah berhasil atau gagal.

SM MO adalah kemampuan dari sistem GSM untuk mentransfer pesan yang dikirim dari MS (*Mobile Station*) ke SME melalui SC, dan juga menyediakan informasi mengenai pengiriman pesan, apakah gagal atau sukses, juga pesan tersebut mengikutsertakan alamat dari SME supaya SC dapat berhasil mengirimkan pesan tersebut.

Sebuah MS yang aktif dapat menerima pesan singkat (*SMS deliver*) setiap saat, sebuah laporan selalu dikirimkan ke SC untuk memberi informasi bahwa MS (*Mobile Station*) sudah menerima pesan, berhasil diterima atau tidak, serta alasannya.

2.5.3 PDU (Protocol Data Unit)

PDU atau Protocol Data Unit adalah bahasa yang digunakan SMS. Data yang mengalir ke/dari SMS-centre harus berbentuk PDU. PDU berisi bilangan-bilangan heksadesimal yang mencerminkan bahasa I/O. PDU terdiri dari beberapa header. Header untuk mengirim SMS ke SMS-centre berbeda dengan SMS yang diterima dari SMS-centre. Maksud dari bilangan heksadesimal adalah bilangan yang terdiri atas 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.



Gambar 2.4 Jaringan Sederhana Teknologi SMS

2.6 Teori Antrian

Menurut Siagian (1987), antrian ialah suatu garis tunggu dari nasabah (satuan) yang memerlukan layanan dari satu atau lebih pelayan (fasilitas layanan). Pada umumnya, sistem antrian dapat diklasifikasikan menjadi sistem yang berbeda – beda di mana teori antrian dan simulasi sering diterapkan secara luas. Klasifikasi menurut Hillier dan Lieberman adalah sebagai berikut :

1. Sistem pelayanan komersial
2. Sistem pelayanan bisnis – industri
3. Sistem pelayanan transportasi
4. Sistem pelayanan sosial

Sistem pelayanan komersial merupakan aplikasi yang sangat luas dari model-model antrian, seperti restoran, kafetaria, toko-toko, salon, butik, supermarket, dan sebagainya. Sistem pelayanan bisnis-industri mencakup lini produksi, sistem material-handling, sistem pergudangan, dan sistem-sistem informasi komputer. Sistem pelayanan sosial merupakan sistem-sistem pelayanan yang dikelola oleh kantor-kantor dan jawatan-jawatan lokal maupun nasional,

seperti kantor registrasi SIM dan STNK, kantor pos, rumah sakit, puskesmas, dan lain-lain (Subagyo, 2000).

2.6.1 Komponen Dasar Antrian

Komponen dasar proses antrian adalah :

1. Kedatangan

Setiap masalah antrian melibatkan kedatangan, misalnya orang, mobil, panggilan telepon untuk dilayani, dan lain – lain. Unsur ini sering dinamakan proses *input*. Proses *input* meliputi sumber kedatangan atau biasa dinamakan *calling population*, dan cara terjadinya kedatangan yang umumnya merupakan variabel acak. Menurut Levin, dkk (2002), variabel acak adalah suatu variabel yang nilainya bisa berapa saja sebagai hasil dari percobaan acak. Variabel acak dapat berupa diskrit atau kontinu. Bila variabel acak hanya dimungkinkan memiliki beberapa nilai saja, maka ia merupakan variabel acak diskrit. Sebaliknya bila nilainya dimungkinkan bervariasi pada rentang tertentu, ia dikenal sebagai variabel acak kontinu.

2. Pelayan

Pelayan atau mekanisme pelayanan dapat terdiri dari satu atau lebih pelayan, atau satu tau lebih fasilitas pelayanan. Tiap – tiap fasilitas pelayanan kadang – kadang disebut sebagai saluran (*channel*) (Schroeder, 1997). Contohnya, jalan tol dapat memiliki beberapa pintu tol. Mekanisme pelayanan dapat hanya terdiri dari satu pelayan dalam satu fasilitas pelayanan yang ditemui pada loket seperti pada penjualan tiket di gedung bioskop.

3. Antri

Inti dari analisa antrian adalah antri itu sendiri. Timbulnya antrian terutama tergantung dari sifat kedatangan dan proses pelayanan. Jika tak ada antrian berarti terdapat pelayan yang menganggur atau kelebihan fasilitas pelayanan (Mulyono, 1991). Penentu antrian lain yang penting adalah disiplin antri. Disiplin antri adalah aturan keputusan yang menjelaskan cara melayani pengantri. Menurut Siagian (1987), ada 5 bentuk disiplin pelayanan yang biasa digunakan, yaitu :

- a. *FirstCome FirstServed (FCFS)* atau *FirstIn FirstOut (FIFO)* artinya, lebih dulu datang (sampai), lebih dulu dilayani (keluar). Misalnya, antrian pada loket pembelian tiket bioskop.
- b. *LastCome FirstServed (LCFS)* atau *LastIn FirstOut (LIFO)* artinya, yang tiba terakhir yang lebih dulu keluar. Misalnya, sistem antrian dalam elevator untuk lantai yang sama.
- c. *Service In Random Order (SIRO)* artinya, panggilan didasarkan pada peluang secara random, tidak soal siapa yang lebih dulu tiba.
- d. *Priority Service (PS)* artinya, prioritas pelayanan diberikan kepada pelanggan yang mempunyai prioritas lebih tinggi dibandingkan dengan pelanggan yang mempunyai prioritas lebih rendah, meskipun yang terakhir ini kemungkinan sudah lebih dahulu tiba dalam garis tunggu. Kejadian seperti ini kemungkinan disebabkan oleh beberapa hal, misalnya seseorang yang dalam keadaan penyakit lebih berat dibanding dengan orang lain dalam suatu tempat praktek dokter

2.6.2 Sistem Antrian dengan Menggunakan Prioritas Pelayanan (*priority service*)

Sistem antrian sering dimodelkan dengan prioritas-prioritas tertentu. Hal ini juga dapat dijumpai pada berbagai bentuk antrian paralel. Suatu antrian paralel dapat berada di depan satu fasilitas pelayanan dan dapat juga berada pada beberapa fasilitas pelayanan dengan prioritas tertentu. Bila pada suatu fasilitas pelayanan terdapat antrian dengan pelanggan yang mempunyai antrian paralel, maka dapat dinyatakan bahwa antrian yang pertama mempunyai prioritas pertama untuk dilayani, sedangkan antrian kedua, termasuk pelanggannya, mempunyai prioritas yang lebih rendah. Prioritas dalam sistem antrian ini dapat ditentukan berdasarkan kebutuhan yang disesuaikan dengan ketentuan yang berlaku.

Pada tingkat kedatangan dapat ditentukan bahwa setiap pelanggan yang berada dalam antrian harus dilayani berdasarkan “yang pertama datang, juga pertama dilayani”(FCFS). Dalam prioritas pelayanan terdapat dua aturan yang dapat diikuti, yaitu:

1. Aturan *Preemptive*

Menunjukkan bahwa pelanggan dengan prioritas pelayanan yang rendah tetap dapat memasuki fasilitas pelayanan bersama-sama dengan pelanggan yang datang pada prioritas yang utama (sangat tinggi).

2. Aturan *Non-Preemptive*

Menunjukkan bahwa bila suatu pelanggan sudah memasuki fasilitas pelayanan maka pelanggan tersebut akan terus dilayani sampai selesai, walaupun datang pelanggan dengan prioritas yang lebih tinggi.

Aturan preemptive umumnya tidak menguraikan sistem antriannya secara mendalam, sedangkan pada sistem antrian non-preemptive diuraikan melalui pelayanan tunggal dan pelayanan majemuk.

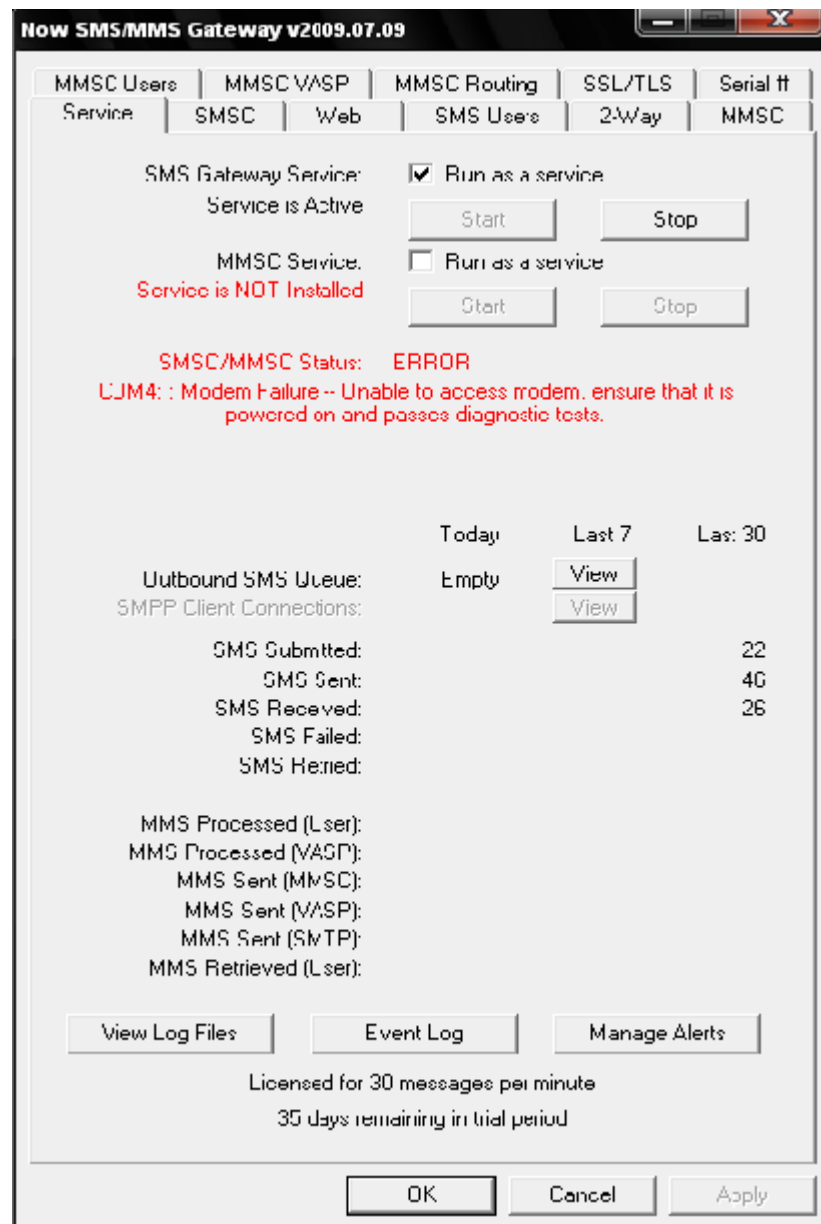
Pada model pelayanan tunggal dapat ditentukan untuk menggunakan distribusi poisson sebagai tingkat kedatangan pada sistem antrian, sementara pelayanan menggunakan distribusi bebas (*arbitrary distribution*).

Pada kasus pelayanan majemuk sudah ditentukan bahwa kedatangan dan pelayanan menggunakan distribusi poisson.

2.7 Now SMS

NowSMS adalah aplikasi yang digunakan sebagai alat untuk memungkinkan pengembangan interaktif cepat aplikasi dan layanan SMS. Ketika NowSMS menerima pesan SMS, dapat dikonfigurasi untuk mengirim pesan ke sebuah script yang menjalankan pada server HTTP. NowSMS ini menyediakan cara sederhana untuk mendapatkan pesan yang diterima ke dalam sebuah aplikasi, sehingga aplikasi dapat melakukan pemrosesan kustom pada pesan, aplikasi ini juga dapat menghasilkan jawaban yang sederhana kembali ke pesan yang diterima.

Berikut adalah gambar yang aplikasi NowSMS yang sudah terinstal:



Gambar 2.5 Aplikasi NowSMS

2.8 Siklus Hidup Pengembangan Sistem (System Development Life Cycle)

Pengembangan sistem informasi berbasis komputer dapat merupakan tugas kompleks yang membutuhkan banyak sumber daya dan dapat memakan waktu berbulan-bulan bahkan bertahun-tahun untuk menyelesaikannya. Proses pengembangan sistem melewati beberapa tahapan dari mulai sistem itu

dienankan sampai dengan sistem tersebut diterapkan, dioperasikan dan dipelihara.

Di *system development life cycle* (SDLC) tiap-tiap bagian dari pengembangan sistem dibagi menjadi beberapa tahapan kerja. Tiap tahapan memiliki karakteristik tersendiri. Tahapan utama siklus hidup pengembangan sistem dapat terdiri dari tahapan perencanaan (*system planning*), analisis sistem (*system analysis*), desain sistem (*system design*), seleksi sistem (*systems selection*), implementasi sistem (*system implementation*) dan perawatan sistem (*system maintenance*). (Jogiyanto, 1999)

Menurut James Taylor (Taylor, 2004) tahapan SDLC meliputi tahapan sebagai berikut:

Tabel 2.1 *System Development Life Cycle*

No	Phase	Activities
1.	Konsep	Mendefinisikan Kebutuhan produk, membangun analisa kemungkinan yang akan terjadi, mendefinisikan <i>scope</i> (batasan) produk, membangun sistem arsitektur
2.	Kebutuhan (<i>requirement</i>)	
3.	Desain	menyelesaikan kebutuhan produk, melengkapi desain secara utuh (<i>preliminary design</i>)
4.	Implementasi	Meminta persetujuan desain dan tanda tangan dari pihak investr, membangun desain secara detail dan membangun system
5.	Integrasi dan tes	Membangun dan menghubungkan unit-unit dalam system, dan uji coba pengintegrasian sistem. Pengiriman sistem (<i>Deliver system</i>).
6.	Instalasi sistem	Instalasi dan uji coba sistem

7.	Pemeliharaan (<i>Maintenance</i>) dan pendukung (<i>support</i>)	Pengoperasian dan pemeliharaan sistem
----	--	---------------------------------------

Fase *concept* dan *requirement* secara garis besar merupakan tahap awal pengembangan sistem yang meliputi pendefinisian kebutuhan produk, mendefinisikan *scope* (batasan) produk serta membangun rancangan arsitektur sistem.

Tahap *design* merupakan suatu proses dimana analisa kebutuhan suatu produk telah benar-benar diketahui dan pada tahap ini desain sistem secara utuh harus dipersiapkan.

Setelah sistem di desain, tahap berikutnya adalah implementasi sistem. Dalam tahap ini, hasil desain sistem akan dibangun secara detail. Hasil implementasi akan diintegrasikan dengan keseluruhan bagian sistem. Dan tahap *testing* / pengujian akan membuktikan keabsahan sistem. Tahap terakhir dari siklus hidup sistem adalah tahap pemeliharaan. Tujuan pemeliharaan adalah agar kesinambungan sistem terjaga.

Sebelum sistem baru dibuat, perencanaan perlu dibuat untuk mendefinisikan kebutuhan. Tahap perencanaan meliputi investigasi awal untuk menentukan *project scope*, *project objective* dan *project methodology*. Project scope (batasan project) yaitu cakupan proyek yang akan dibuat. Project objective (objek dari suatu project) muncul karena adanya permasalahan terhadap sistem yang telah ada. Metodologi project (*project methodology*) yang merupakan pedoman tentang bagaimana dan apa yang harus dikerjakan selama pengembangan sistem.

Analisa kebutuhan sistem mencakup pengumpulan dan analisa informasi yang dibutuhkan untuk pengembangan sistem selanjutnya. Hal yang dilakukan pada tahap ini yaitu:

1. Identifikasi kembali masalah (*redefine the problem*)
2. Mengidentifikasi dan memahami sistem yang telah ada
3. Identifikasi dan mendefenisikan kebutuhan pengguna dan hambatan yang mungkin ditemui pada sistem baru

Tahap perancangan merupakan tahapan dimana kebutuhan suatu sistem telah jelas teridentifikasi, sehingga pada bagian ini akan dihasilkan prototipe dari sistem yang akan dibuat. Tahapan yang dilalui meliputi:

1. Identifikasi secara jelas kebutuhan sistem
2. Identifikasi *hardware* dan *software* yang dibutuhkan dalam implementasi sistem
3. Perancangan *interface*
4. Perancangan *database*

Setelah itu, tahap implementasi akan mengkonversikan prototipe dan hasil perancangan sebelumnya dalam bahasa pemrograman. Dalam tahap inilah, sistem informasi benar-benar dibangun. Tahap implementasi juga mencakup instalasi dan *coding*.

Pengujian merupakan tahap terpenting setelah sistem informasi selesai dibuat. Tahap pengujian dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan satu kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan

Hasil pengujian yang telah berhasil akan dianalisa kembali pada bagian analisa akhir untuk mendapatkan hasil yang benar-benar valid dan akurat. Kegagalan pada tahap pengujian akan berakibat lambatnya penyelesaian suatu sistem karena sistem akan dianalisa ulang dari awal untuk mengetahui kesalahan identifikasi.

2.9 *System Development Methodology*

System Development Methodology (Metodologi pengembangan sistem) adalah suatu kerangka kerja yang digunakan untuk menyusun, merencanakan dan mengontrol proses pengembangan suatu system informasi. Metodologi adalah kesatuan metode-metode, prosedur-prosedur, konsep-konsep pekerjaan, aturan-aturan dan postulat-postulat yang digunakan oleh suatu ilmu pengetahuan, seni atau disiplin lainnya. (Jogiyanto,1999)

Menurut Jogiyanto (1999) metodologi pengembangan sistem ada 3 sebagaimana dijelaskan pada sub bab berikut:

2.9.1 System Development Methodology *Functional Decomposition methodologies.*

Metodologi menekankan pada pemecahan dari system ke dalam sub system yang lebih kecil, sehingga akan lebih mudah untuk dipahami, dirancang dan diterapkan. Yang termasuk adalah kelompok ini adalah:

- a. HIPO (*Hierarchy Plus Input Process Output*)
- b. *Stepwise refinement* (SR) atau *iterative Stepwise refinement* (ISR)

2.9.2 *Data Oriented methodologies*

Metodologi ini menekankan pada karakteristik dari data yang akan diprses.

Metodologi ini dikelompokkan lagi kedalam dua kelas, yaitu

2.9.2.1 *Data flow oriented methodologies*

Metodologi ini secara umum didasarkan pada pemecahan dari system ke dalam modul-modul berdasarkan tipe elemen data dan tingkah laku logika mdul tersebut didalam system. Dalam metodologiini, system secara logika dapat digambarkan secara logika dari arus data dan hubungn antar fungsinya di dalam modul-mdul di system. Yang termasuk dalam metdologi ini adalah:

- a. SADT (*Structured analysis and design techniques*)
- b. *Composite design*
- c. *Structured Systems analysis and Design (SSAD)*

2.9.2.2 *Data structure oriented methodologies*

Metodologi ini menekankan pada struktur input dan output di system. Struktur ini kemudian akan digunakan sebagai dasar struktur dari sistemnya. Hubungan fungsi antar modul atau elemen system kemudian dijelaskan dari struktur sistemnya. Yang termasuk metodologi ini adalah:

- a. JSD (*Jackson's system development*)
- b. W/O (warnier /Orr)

2.9.3 *Prescriptive methodologies*

Yang termasuk metodologi ini adalah:

- a. ISDOS (*Informatin system and optimation system*)
- b. PLEXSYS

Kegunaan PLEXSYS adalah untuk melakukan transformasi suatu statement bahasa komputer tingkat tinggi ke suatu *executable code* untuk suatu konfigurasi perangkat keras yang diinginkan

c. PRIDE

Ditawarkan oleh suatu perusahaan di Amerika Serikat yaitu M Bryce & Associates

Dengan demikian dapat dinyatakan bahwa $(M_i/G_i/1):(NP/\infty/\infty)$ yang dapat diartikan dengan :

M_i = kedatangan mengikuti distribusi poisson

G_i = pelayanan mengikuti distribusi bebas (arbitrary)

2.4.2.1 Pelayanan Tunggal N-P

Pelayanan tunggal dengan aturan non-preemptive dikenal dengan simbol $(M_i/G_i/1):(GD/NP/\infty/)$. Model pelayanan ini mengikuti sistem pelayanan dengan distribusi bebas.

Dinyatakan $F_i(t)$ sebagai fungsi kumulatif dari distribusi bebas pada waktu pelayanan pada antrian ke-I untuk $i = 1, 2, \dots, m$.

Bila rata-rata (mean) = $E_i(t)$, dengan $\text{var}_i(t)$ sebagai varian dan λ_i merupakan tingkat kedatangan dari antrian ke-I per unit waktu, maka juga akan terdapat antrian dalam rangkaian sistem antrian tersebut.

Perumusan yang diuraikan dalam sistem antrian pada umumnya dinyatakan sebagai berikut :

1. Ekspektasi dari jumlah pelanggan dalam sistem antrian dengan sebanyak k antrian dinyatakan dengan:

$$L_s(k) = L_q(k) + P_k \quad \dots\dots\dots \text{II-1}$$

2. ekspektasi dari jumlah pelanggan dalam antrian pada sebanyak k antrian dinyatakan dengan :

$$L_q(k) = \lambda_k \cdot W_q(k) \quad \dots\dots\dots \text{II-2}$$

3. ekspektasi waktu menunggu daripada pelanggan dalam antrian dengan sebanyak k antrian dinyatakan dengan:

$$W_q(k) = \frac{\sum_{i=1}^m \lambda_i (E_i^2(t) + \text{var}_i(t))}{2(1-s_k-1)(1-s_k)} \dots\dots\dots \text{II-3}$$

4. ekspektasi waktu menunggu dari pada pelanggan dalam sistem antrian dengan sebanyak k-antrian dapat dirumuskan seagai berikut:

$$W_s(k) = W_q(k) + E_k(t) \dots\dots\dots \text{II-4}$$

Dengan pernyataan yang ditunjukkan dengan pada :

- $P_k = \lambda_k \cdot E_k(t)$
- $S_k = \sum_{i=1}^k \rho_i < 1$ untuk $k=1,2,3,,m$
- $S_0 = 0$

Dari semua perumusan ini akan dapat diperoleh W_q sebagai ekspektasi waktu menunggu di dalam antrian untuk setiap pelanggan dengan prioritas masing-masing, dapat dirumuskan melalui :

$$W_q = \sum_{i=1}^m \frac{\lambda_k}{\lambda} \cdot W_q(k)$$

Dengan pernyataan :

- $\lambda = \sum_{i=1}^k \lambda_i$
- λ_k = berat relative dari $W_q(k)$

Demikian juga hal yang sama dapat dilakukan pada W_s

2.4.2.2 Pelayanan Majemuk N-P

Pelayanan majemuk dengan aturan Non- preemptive dikenal dengan simbol $(M/M/C) : (NP/\infty/\infty)$, merupakan model untuk semua pelanggan mendapatkan distribusi waktu pelayanan yang sesuai dengan probabilitasnya.

Semua fasilitas pelayanan c akan mengikuti distribusi pelayanan yang identik dengan distribusi eksponensial dengan tingkat rata-rata pelayanan μ . Sedangkan kedatangan pada antrian dengan k prioritas akan mengikuti distribusi poisson pada suatu tingkat rata-rata kedatangan λ_k untuk $k=1,2,\dots,m$ dan dapat dinyatakan untuk sejumlah k -antrian yang dirumuskan sebagai ekspektasi waktu menunggu berikut ini:

$$1. W_q(k) = \frac{E(E_0)}{(1-S_{k-1})(1-S_k)} \dots\dots\dots \text{II-5}$$

Untuk $k=1,2,\dots,m$

Dimana :

- $S_0 = 0$
- $S_k = \sum_{i=1}^m \frac{\lambda_i}{S_k} < 1$
- $E(E_0) = \mu \cdot c [p^c(c-p)(c-1)! \sum_{n=0}^{c-1} \frac{\rho^n}{n!} + 1]^{-1}$

Untuk semua $\rho = \lambda/\mu$

2. Ekspektasi waktu pelanggan menunggu didalam antrian untuk sistem antrian parallel dinyatakan dengan rumus :

$$W_q = \sum_{i=1}^k \frac{\lambda_i}{\lambda} \cdot W_q(k) \dots\dots\dots \text{II-6}$$

3. Ekspektasi jumlah pelanggan yang menunggu untuk semua antrian parallel dinyatakan dengan rumus:

$$L_q = \lambda \cdot W_q \rightarrow \text{untuk : } \lambda = \sum_{i=1}^k \lambda_i \dots\dots\dots \text{II-7}$$

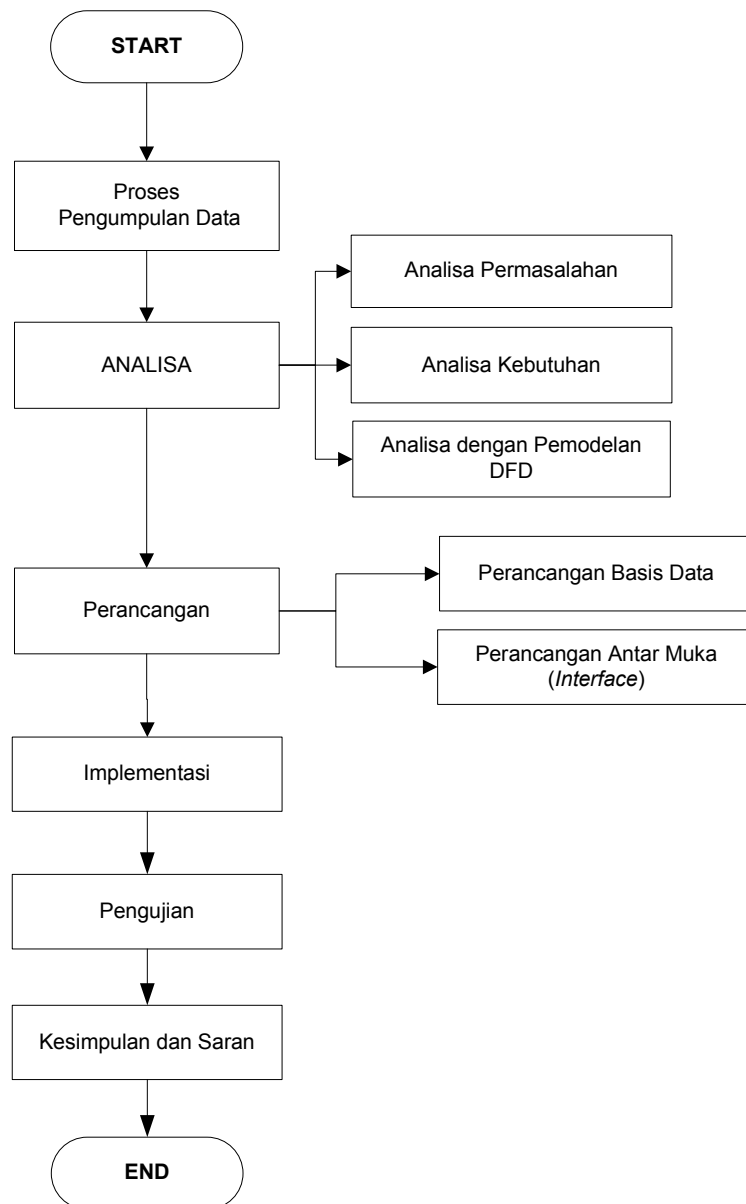
Dengan demikian tampak bahwa ketiga formula yang menjelaskan sistem antrian pelanggan secara parallel dengan pelayanan majemuk, dan juga dengan aturan *non preempative*, sangat berguna untuk menyelesaikan berbagai persoalan dalam kehidupan nyata.

- e. *Squid DNS Statistics*
- f. *Squid Error Rate*
- g. *Squid Number of Clients*
- h. *Squid Page Faults*
- i. *Squid Service Timers*
- j. *Squid Storage Activity*
- k. *Squid Storage Utilisation*
- l. *Squid Traffic In / Out / Saved*

BAB III

METODOLOGI PENELITIAN

Metodologi penelitian merupakan sistematika tahapan penelitian yang dilakukan selama pembuatan tugas akhir. Tahapan yang dilakukan tersebut tertuang pada gambar 3.1 berikut ini.



Gambar 3.1 Siklus Hidup Pengembangan Sistem

Metodologi penelitian yang akan dilakukan berdasarkan Gambar 3.1 meliputi beberapa prosedur-prosedur pengerjaan dan secara garis besar melalui enam tahapan yaitu :

3.1 Pengumpulan Data

Pengumpulan data merupakan tahapan persiapan yang harus dilaksanakan terlebih dahulu sebelum dilakukan penelitian. Berikut merupakan aktivitas yang dilaksanakan dalam pengumpulan data :

1. Studi Pustaka

Studi pustaka berfungsi untuk mendukung penelitian yang akan dilaksanakan. Pengumpulan teori-teori yang mendukung dalam penelitian ini merupakan kegiatan dalam studi pustaka. Teori-teori bersumber dari buku, jurnal dan penelitian-penelitian sejenis.

2. Wawancara

Wawancara berfungsi untuk mengumpulkan informasi yang akan berguna untuk tahap analisa dan tahap-tahap selanjutnya. Wawancara dilakukan terhadap praktisi jaringan

3.2 Analisa

Tahapan selanjutnya adalah melakukan analisa. Analisa merupakan suatu proses yang berguna untuk melakukan pemilahan pada apa yang akan dikerjakan. Kemudian dilanjutkan pada perancangan sistem berdasarkan dari analisa permasalahan sebelumnya. Proses ini terbagi menjadi tiga tahapan :

3.2.1 Analisa Permasalahan Sistem Lama

Bagian awal dari Bab Analisa membahas tentang sistem lama yakni CACTI yang masih murni tanpa tambahan fitur. Bagian ini mencakup semua hal yang menjadi bagian dari instalasi, penggunaan, cara kerja CACTI, proses alert serta kelemahan dan kekurangan alert yang dikeluarkan CACTI. Kemudian, disini juga mencakup bagaimana solusi yang mungkin untuk mengatasi kekurangan tersebut.

3.2.2 Analisa Kebutuhan Sistem Baru

Setelah sistem lama dianalisa, maka akan muncul kebutuhan untuk membangun sistem baru, kebutuhan itu mengacu pada apa yang menjadi kekurangan pada keluaran alert yang dihasilkan CACTI. Analisa kebutuhan yang dimaksud meliputi analisa kebutuhan data, analisa kebutuhan perangkat, analisa dan kebutuhan fungsi

3.2.3 Analisa dengan Pemodelan DFD

Untuk analisa fungsional, dalam tugas akhir ini akan digunakan metodologi analisa dan desain sistem secara terstruktur (*Structured Systems analysis and Design*) karena metodologi ini menggunakan pendekatan pengembangan system secara terstruktur. *Tools* atau alat Bantu yang akan digunakan adalah data flow diagram (DFD). Bagian ini merupakan bagian penentu untuk melangkah pada bagian selanjutnya karena logika aliran data dianalisa pada bagian ini. Kesalahan pada bagian ini dapat berakibat fatal karena akan mengubah sistem yang akan dibuat. Hasil pada bagian ini akan digunakan untuk melakukan perancangan.

3.3 Perancangan

Tahap perancangan sistem merupakan prosedur untuk mengkonversi spesifikasi logis kedalam sebuah perancangan yang dapat diimplementasikan pada perangkat lunak. Perancangan yang akan dibuat meliputi perancangan basis data dan perancangan antarmuka. Keduanya dikembangkan berdasarkan hasil analisa yang telah dilakukan

3.3.1 Perancangan Basis Data

Setelah menganalisa bagaimana sistem yang akan dibuat maka dilakukan perancangan basis data untuk melengkapi komponen sistem. Perancangan meliputi perancangan tabel yang akan digunakan oleh sistem. Seluruh tabel merupakan representasi dari *data store* yang ada pada bagian analisa dengan DFD.

3.3.2 Perancangan Antar Muka

Sementara untuk perancangan antarmuka merupakan reka bentuk tampilan dari sistem yang akan dibuat. Antarmuka terdiri dari rancangan struktur menu dan rancangan tampilan, yang akan dibuat sesuai dengan kebutuhan masing-masing fungsi.

3.4 Implementasi

Implementasi pengembangan sistem ini dilaksanakan dengan menggunakan bahasa pemrograman PHP dan database My SQL. Pada implementasi berisi juga tentang alasan pemilihan perangkat lunak beserta batasan implementasi dan lingkungan implementasi. Kebutuhan untuk membangun perangkat lunak adalah:

1. Kebutuhan Perangkat Keras (*Hardware*)

Perangkat keras yang dibutuhkan untuk membangun system yaitu:

- a. Personal computer dengan prosesor Pentium 4 atau di atasnya
- b. 512 MB RAM
- c. Hard disk dengan kapasitas 40 GB
- d. modem, berupa perangkat telepon genggam GSM beserta *simcard*
- e. kabel DKU 5

2. Kebutuhan Perangkat Lunak (*Software Requirements*)

Pemilihan software untuk tugas akhir ini akan melibatkan banyak aspek yaitu:

- a. *Software* tersebut harus memiliki *user interface* yang menarik
- b. *Software* tersebut harus bisa berinteraksi dengan *database*
- c. *Software* tersebut harus berbasis web dan bersifat *open source*

Beberapa *hardware* dan *software* dibutuhkan untuk menunjang pengembangan system serta eksekusi system yang efisien, sistematis dan efektif. Table 3.1 menunjukkan *software* yang dibutuhkan untuk membangun system. Berikut ini adalah daftar software yang dibutuhkan untuk menunjang implementasi sistem:.

Table 3.1 : Kebutuhan Perangkat Lunak untuk Membangun Sistem

Software	Purpose
Cacti dan <i>software</i> pendukungnya, yaitu: RRD Tool, Net SNMP, Thold dan spine NowSMS gateway	<i>Software</i> monitoring yang akan diinstalasi

Microsoft Office Visio 2003	Digunakan untuk menggambar diagram.
PHP 5	Ini adalah bahasa pemrograman yang akan digunakan untuk membangun system
Apache Server	Sebagai <i>web server</i> untuk menjalankan sistem.
Microsoft Windows XP	Sistem operasi tempat sistem diimplementasikan
MySQL database	Untuk menyimpan semua data yang dibutuhkan system
Microsoft Words 2003	Sebagai <i>platform</i> yang digunakan untuk mendokumentasikan seluruh pekerjaan

Setelah dilaksanakan implementasi, maka akan dilakukan pengujian terhadap implementasi yang telah dilaksanakan dan tinjauan ulang terhadap unjuk kerja sistem.

3.5 Pengujian

Pada tahapan pengujian ini menggambarkan kondisi-kondisi yang terjadi apabila aplikasi dijalankan. Standar pengujian yang dilakukan berkaitan dengan uji fitur dan hasil pengiriman SMS notifikasi, apakah sesuai dengan yang diharapkan.

3.6 Kesimpulan dan Saran

Hasil dari pengujian akan dikaji dan dianalisa ulang untuk mendapatkan hasil yang benar-benar diharapkan. Kesimpulan, kekurangan dan saran pengembangan sistem akan diletakkan pada bagian kesimpulan dan saran.

BAB IV

ANALISA DAN PERANCANGAN

Analisa ialah suatu proses identifikasi permasalahan dari kumpulan data yang bernilai informasi dan bermanfaat pada pembangunan sistem. Analisa merupakan langkah awal dalam membuat suatu aplikasi. Analisa dilakukan untuk memahami persoalan sebelum melakukan tahap perancangan. Hal ini dilakukan untuk mencari kebutuhan-kebutuhan yang diperlukan oleh sistem dan kendala-kendala yang akan dicari solusinya. Setelah analisa dilakukan, tahap selanjutnya adalah perancangan sistem. Perancangan yang dibuat harus memiliki kesesuaian dengan analisa sistem yang sebelumnya telah dilakukan.

4.1. Analisa Sistem yang Sedang Berjalan

CACTI merupakan salah satu *Network Monitoring System* yang bekerja berdasarkan konsep SNMP pada pengumpulan informasi statistik jaringan. CACTI adalah *frontend* dari RRDTool yang menyimpan informasi kedalam basis data MySQL dan membuat grafik berdasarkan informasi tersebut. Proses pengambilan data (lewat SNMP maupun skrip) sampai kepada pembuatan grafik dilakukan menggunakan bahasa pemrograman PHP.

Kebutuhan awal sebelum instalasi CACTI yaitu Web Server (Apache), PHP (PHP 5), Basis data MySQL (MySQL 5), Net-SNMP dan paket RRDTool. Untuk proses instalasi CACTI dapat dilihat selanjutnya pada Lampiran A.

Secara umum cara kerja CACTI dapat digambarkan sebagai berikut:

- a. Data Retrieval

Hal pertama yang dilakukan oleh CACTI adalah mengumpulkan data. Data dikumpulkan dengan Poller yang dieksekusi oleh sistem operasi. Interval pengumpulan data atau dengan kata lain eksekusi Poller dapat diatur melalui fasilitas penjadwalan yang tersedia di Operating System. Data yang telah tersedia di *host* atau remote target dapat didapatkan dengan *Simple Network Management Protocol* (SNMP). Sehingga tiap perangkat yang dapat menjalankan fungsi SNMP (*managed agents/nodes*) dapat dimonitoring secara bersamaan oleh CACTI

b. Data Storage

Data yang telah dikumpulkan oleh Poller, selanjutnya akan disimpan secara teratur di bawah folder */rra*. Untuk proses ini, CACTI menggunakan Round Robin Database (RRD) dimana data akan ditata dalam urutan waktu (*time-series*). Data yang dapat berupa trafik jaringan, suhu mesin, *server load average*, *mounting load* dan lainnya berbentuk file berekstensi *.rra* dan selanjutnya siap dipresentasikan dalam bentuk grafik.

c. Data Presentation

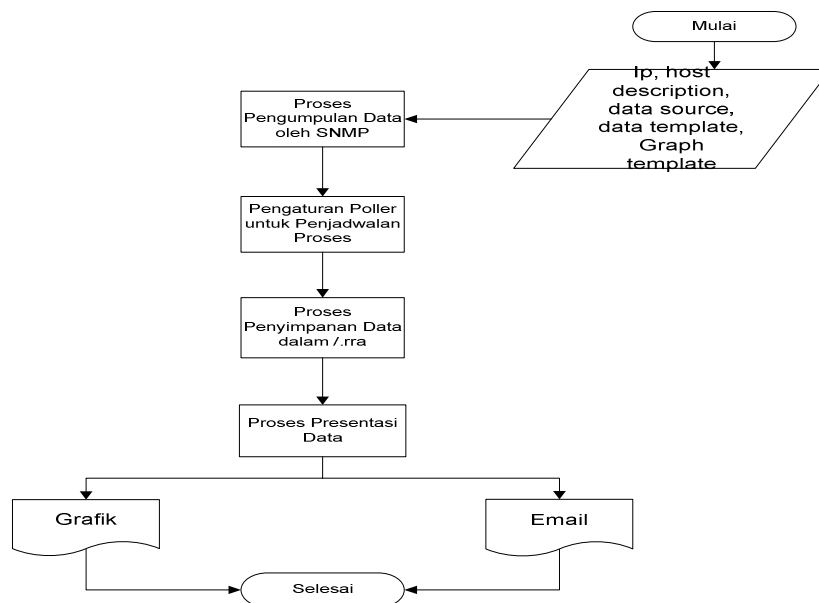
Keutamaan penggunaan RRDtool adalah fungsi grafiknya. Data-data yang tertata dalam folder */rra* akan di presentasikan dalam grafik dan ditampilkan oleh webserver yang digunakan. CACTI juga menyediakan halaman pengaturan grafik untuk memudahkan manajemen gambar-gambar yang ingin ditampilkan serta cara menampilkannya.

Interval poller yang dimiliki CACTI memiliki nilai default 5 menit (300 detik). Poller 5 menit merupakan batas awal penentuan poller oleh kontributor

CACTI karena 5 menit merupakan waktu yang paling optimal untuk melakukan event pada monitoring jaringan. Secara default, dalam 5 menit CACTI akan melakukan *refresh* dan pengumpulan kembali nilai statistik jaringan. Nilai ini juga akan disertai dengan perubahan dan penyimpanan grafik setiap 5 menitnya, oleh sebab itu nilai di bawah 5 menit belum dapat dilakukan karena tidak optimal dari segi pemakaian memori pada CACTI server itu sendiri.

Dalam perkembangannya, CACTI mampu memberikan keluaran dalam bentuk *email*. *Email* yang dihasilkan merupakan sebuah pesan peringatan akan adanya suatu kerusakan ataupun masalah dalam jaringan. Fasilitas ini tersedia apabila *plugin* THOLD diinstalasikan bersamaan dengan modul CACTI. Pengaturan dan instalasi mengenai hal tersebut dapat dilihat dalam lampiran B

Secara umum proses pemantauan oleh CACTI dapat dilihat pada gambar 4.1.



Gambar 4.1 Flowchart Proses Pengumpulan Statistik Jaringan Oleh CACTI

Layaknya sistem monitoring lainnya, CACTI memiliki banyak kelebihan sekaligus kekurangan. Kelebihan CACTI antara lain:

1. Dari segi biaya, CACTI bersifat *open source* (gratis biaya lisensi) sehingga modul CACTI dapat dengan mudah diunduh dan digunakan oleh siapa saja.
2. Dibandingkan dengan MRTG yang juga bersifat *open source*, tampilan CACTI jauh lebih menarik dan fiturnya lebih lengkap
3. Sebagai sistem monitoring, CACTI cukup handal untuk dapat memonitoring aktifitas dan peralatan yang ada di jaringan
4. CACTI juga sudah mendukung SNMP versi 2 dan versi 2c dengan enkripsi MD5, dengan demikian dari segi keamanan, CACTI sudah memenuhi standar keamanan enkripsi data

Masih termasuk dalam kelebihan CACTI, dalam pengumpulan data dan informasi statistik jaringan, CACTI menggunakan pilihan protokol SNMP dan ICMP sekaligus sehingga saling menutupi masing-masing protokol dalam hal monitoring. Artinya, beberapa hal yang tidak dapat didukung oleh protokol ICMP akan dilengkapi oleh protokol SNMP, begitu juga sebaliknya. Dalam proses presentasi hasil monitoring, CACTI menampilkannya dalam bentuk grafik. Masing-masing *host* yang telah di daftarkan untuk dimonitor, secara langsung akan memiliki hasil statistik dalam bentuk grafik.

Pilihan untuk memunculkan alert tersedia dalam CACTI melalui plugin THOLD. Pesan peringatan yang muncul dikeluarkan dalam bentuk *email*. Pesan

peringatan ini muncul apabila data statistik jaringan pada suatu waktu melebihi ambang batas (threshold) yang telah ditetapkan.

Meskipun CACTI memiliki banyak fitur dengan berbagai kelebihan, tetap saja CACTI masih memiliki keterbatasan, misalkan untuk kasus yang membutuhkan reliabilitas (kehandalan) tinggi dimana perlu adanya ketersediaan informasi saat administrator berada dimanapun, CACTI belum menyediakan fasilitas tersebut. Selain itu, beberapa *data template*, *data source*, dan *grafik template* hanya *compatible* dengan *host* jaringan dari merek dan vendor tertentu. Disamping CACTI juga belum mampu untuk menangani trouble shooting jaringan secara langsung, dalam arti bahwa CACTI adalah murni *tools* untuk monitoring dan belum menyertakan fasilitas untuk *trouble shooting* masalah jaringan dalam modulnya. Oleh sebab itu, tugas akhir ini akan mencoba menutupi kekurangan CACTI yakni penambahan fitur CACTI dalam hal penyediaan informasi yang lebih fleksibel dan reliabel, pembahasan mengenai hal tersebut akan dijabarkan dalam analisa selanjutnya.

4.2. Analisa Sistem Yang Akan Dibangun

Telah dijelaskan sebelumnya dalam tugas akhir ini akan dibangun fitur baru untuk CACTI yang akan menyempurnakan fitur yang telah ada. Bagian ini akan menganalisa permasalahan pada CACTI sebelum ditambahkan fitur baru berupa SMS, kemudian juga akan dibahas mengenai permasalahan jaringan secara umum untuk mengetahui beberapa permasalahan pada jaringan yang akan digunakan sebagai acuan penyusunan kategori prioritas masalah jaringan itu sendiri. Setelah itu, akan dianalisa perangkat lunak yang akan dibangun.

4.2.1. Analisa Permasalahan CACTI Tanpa Fitur SMS

Banyak hal yang menjadi alasan mengapa CACTI perlu penyempurnaan fitur. Pada bagian ini akan dianalisa permasalahan yang ada pada CACTI yang lama untuk kemudian dijadikan sebagai acuan pada analisa sistem yang akan dikembangkan.

Seorang administrator jaringan memiliki tugas yang amat berat terkait pengumpulan data statistik jaringan apabila dilakukan secara manual. Terlebih untuk kategori jaringan komputer yang memiliki peran penting yang menyangkut keberlangsungan bisnis suatu perusahaan, sehingga diperlukan bantuan sistem yang dapat memberikan informasi mengenai statistik jaringannya. Disamping itu, pada kondisi dimana terjadinya masalah pada jaringan, hal ini juga menjadi tanggung jawab administrator. Informasi mengenai permasalahan jaringan secara langsung memiliki dampak pada proses pemulihan jaringan itu sendiri. Semakin cepat informasi tersebut diperoleh, maka proses pemulihan akan semakin cepat pula ditanggulangi.

CACTI, sebagai salah satu *network monitoring system* (NMS) memiliki kemampuan untuk mengumpulkan statistik jaringan secara akurat dalam suatu waktu. CACTI juga memiliki kemampuan untuk memberikan pesan peringatan disaat kondisi jaringan sedang bermasalah. Pesan peringatan tersebut dikirimkan dalam bentuk surat elektronik(*electronic mail*). *Email* yang dikirimkan kepada administrator berisi pesan peringatan akan adanya kesalahan pada jaringan, yang dalam hal ini terjadi apabila kondisi statistik jaringan pada suatu waktu melebihi nilai ambang batas yang telah ditetapkan.

Memang notifikasi dengan *email* cukup membantu, terutama untuk pelaporan kepada pihak manajemen yang lebih tinggi. Fasilitas ini akan memberikan informasi kepada administrator yang juga sedang terhubung dengan jaringan tersebut, ataupun minimal memiliki akses dengan media internet untuk dapat menerima pesan masalah jaringan melalui *email*. Namun dibalik itu, masih terdapat kekurangan pada cara pengiriman pesan dengan menggunakan *email*, yaitu:

1. Penerima pesan harus terhubung dengan internet
2. Pesan yang dikirimkan lewat *email* adalah pesan peringatan yang juga disertai grafik hasil monitoring sehingga berukuran besar, dengan demikian waktu yang digunakan untuk membuka pesan *email* cukup lama
3. Seorang *network administrator* harus mengetahui pesan peringatan dalam waktu yang seminimal mungkin mengingat jika ada permasalahan jaringan yang berat, informasi mengenai hal itu harus diketahui secara cepat dan akurat untuk mengembalikan kondisi jaringan pada keadaan semula, dengan demikian *email* tidak cukup cepat untuk menangani hal tersebut
4. Fasilitas *email* hanya didukung oleh beberapa jenis telepon seluler
5. Jika fasilitas *email* diakses menggunakan media telepon seluler (untuk selanjutnya disebut HP/ *handphone*), biayanya relatif mahal dan waktu akses yang semakin lama mengingat *email* menyertakan file berbentuk gambar/ grafik didalamnya (*graph embeded*).

Perbandingannya bila CACTI menggunakan media SMS sebagai penyampai pesan notifikasi masalah jaringan adalah:

1. Berkaitan dengan penggunaan SMS dalam rancang bangun FiCtiMS ini sungguh beralasan; pertama, karena fitur SMS sudah sangat familiar, penggunaannya pun mudah.
2. Kedua, *reliable* dengan semua jenis HP tanpa terkecuali dan tentu saja penggunaan pulasanya jauh lebih murah dibandingkan fitur lainnya seperti MMS (*Multimedia Message Service*).
3. Pengoperasian SMS relatif lebih mudah dan lebih cepat dibandingkan *email*

Oleh sebab itu, pertimbangan akan dibangunnya fitur baru berbasis SMS yang melengkapi fitur CACTI diharapkan dapat menjadi suatu solusi bagi permasalahan yang ada.

4.2.2. Analisa Penggunaan *Priority Service* dalam FiCtiMS (Fitur CACTI berbasis SMS)

Pada subbab 2.2 telah disebutkan beragam contoh permasalahan yang terjadi di jaringan. Pada bagian ini akan dijelaskan kaitan antara perlunya pengelompokan permasalahan tersebut dengan *priority service* serta kaitan dan pengaruh *priority service* pada rancang bangun FiCtiMS yang akan dibuat.

Priority service merupakan suatu pelayanan yang diberikan dalam antrian sesuai dengan urutan prioritas, dimana pelanggan yang memiliki prioritas tertinggi akan dilayani terlebih dahulu.

Terlalu banyaknya masalah pada jaringan serta tidak adanya pengelompokan akan mengakibatkan sulitnya *network administrator* untuk menangani perbaikan terhadap dampak yang ditimbulkan. Hal ini jelas karena

masing-masing masalah jaringan memiliki kategori yang berbeda-beda dengan dampak dan proses penanganan yang berbeda pula. Masalah yang berat perlu penanganan sesegera mungkin untuk menghindari kerusakan yang lebih parah yang mungkin dapat terjadi, sementara masalah jaringan yang ringan dapat ditunda penanganannya bila dinilai tidak membawa pengaruh terlalu besar terhadap sistem.

Kesimpulannya, *priority service* akan digunakan untuk mengelompokkan masalah berdasarkan urutan / kategori prioritasnya sehingga pesan yang terkirim ke administrator adalah benar-benar pesan yang berguna untuk menotifikasi masalah sesuai dengan urutan prioritasnya, dimana masalah yang berat akan mendapatkan prioritas untuk dinotifikasi terlebih dahulu dibandingkan dengan masalah yang ringan.

Pertimbangan penggunaan *priority service* dalam metode pengiriman pesan ke telepon seluler milik administrator adalah :

1. Dengan adanya metode ini pesan yang terkirim kepada administrator dapat dipastikan hanyalah pesan-pesan yang berisi notifikasi permasalahan jaringan yang genting
2. dengan menggunakan *priority service* proses identifikasi masalah jaringan secara satu persatu tidak perlu dilakukan karena informasi permasalahan pada jaringan tersedia lebih jelas dan rinci, dengan demikian proses *troubleshooting* jaringan menjadi lebih cepat

3. masing-masing HP memiliki keterbatasan dalam menerima/ mengirim SMS, untuk itu perlu *priority service* agar kemampuan HP dapat digunakan secara optimal

Selain itu, masing-masing telepon seluler memiliki keterbatasan dalam menerima dan mengirimkan SMS. Dapat dibayangkan apabila pada suatu waktu terdapat 1000 pesan yang berisi masalah dalam jaringan dengan kriteria berbeda, tanpa metode *priority service* seluruh pesan tersebut akan dikirimkan tanpa kecuali. Otomatis, beberapa tipe HP yang memiliki kemampuan dibawah itu akan *hang* seketika setelah menerima ribuan pesan tersebut.

Bila diperhitungkan dari segi waktu, tentu pengiriman SMS tanpa *priority service* juga tidak efektif karena tiap SMS *gateway* juga punya keterbatasan untuk *mem-broadcast* / mengirimkan pesan sekaligus. Sebagai contoh NowSMS *gateway* yang digunakan dalam tugas akhir ini hanya mempunyai kemampuan untuk mengirimkan 6 SMS dalam 1 detik, dimana untuk sampai ke HP tujuan diperkirakan tiap SMS membutuhkan waktu 6 detik per SMS.

Dari seluruh penjelasan yang telah penulis paparkan sebelumnya, itulah mengapa perlu diterapkan metode *priority service* dalam pembagian masalah jaringan sekaligus pengiriman pesannya. Pada bab I sebelumnya penulis telah memaparkan pembagian level skalabilitas dari ancaman menurut Roger S. Pressman (Pressman, 2005) yang di definisikan dalam 4 kategori yakni level bencana (*Catastrophics*), level krisis (*Critical*), level kecil (*marginal*), dan dapat diabaikan (*negligible*).

Dengan alasan untuk lebih mempermudah proses pengiriman pesan, setelah dianalisa penulis membagi beragam permasalahan jaringan tersebut ke dalam 3 kategori risiko saja, yakni *high risk*, *medium risk* dan *low risk*. Penulis mendefenisikan kategori *high risk* sebagai masalah pada jaringan yang memiliki resiko tertinggi terhadap jaringan. Bila dikaitkan dengan pembagian resiko menurut Roger Pressman maka ini berhubungan dengan kategori *catastrophics* dimana akibat yang ditimbulkan mengakibatkan jaringan tidak dapat digunakan. Sementara *medium risk* berhubungan dengan level *critical* dan *low risk* berhubungan dengan level *marginal*. Untuk level *negligible* penulis anggap tidak termasuk dalam kategori resiko karena tidak membawa dampak apapun pada jaringan dan dapat diabaikan.

Penulis membagi level resiko berdasarkan kriteria jenis *host*, waktu pengamatan, dan nilai ambang batas yang telah ditetapkan pada *threshold*. Untuk kriteria jenis *host*, penulis mengelompokkan beberapa *host* yang menjadi prioritas laporan bila terjadi masalah, *host* tersebut adalah *host* yang memiliki peran penting di jaringan seperti *host* yang berada pada server farm, misalkan *DHCP server*, *log server*, *Radius server*, *mail server*, *DNS server*, dan *NMS server* itu sendiri, kemudian *host* yang memiliki tugas mengatur routing pada jaringan yakni router. Ketika *host-host* tersebut mati (statusnya *down*) maka sistem akan secara otomatis memprioritaskan pengiriman pesan peringatan kepada administrator.

Untuk kriteria waktu pengamatan, penulis menganalisa bahwa pada suatu waktu tertentu misalkan pada saat libur ataupun *after hour* (setelah jam kerja) jika terdapat pemakaian jaringan yang melebihi pemakaian pada saat jam kerja

ataupun sama dengan jam kerja, maka dapat dipastikan telah terjadi sabotase atau pemakaian *resource* (sumber daya pada jaringan) yang tidak terotorisasi.

Terakhir untuk kriteria nilai ambang batas (*threshold*), masing-masing batasan kategori resiko adalah 70% untuk kategori high risk, 40 % untuk medium risk dan 10 % untuk low risk (Hendradhy, 2009)

Dari hasil analisa yang penulis paparkan, itu semua bukanlah harga mutlak untuk menjadi dasar pengelompokan kategori masalah dan resiko pada jaringan karena bagaimanapun semua akan kembali lagi pada *policy* yang ditetapkan oleh masing-masing perusahaan, karena ukuran kategori prioritas masalah jaringan tergantung pada servis yang ditangani perusahaan , sebagai contoh perusahaan yang mementingkan transfer data terutama data-data keuangan (misalkan bank) maka hal yang paling menjadi prioritas oleh perusahaan adalah menjaga agar akses ke jaringan yang menangani masalah transaksi *online* selalu terjaga. Begitu pula dengan adanya kepentingan yang berbeda yang dimiliki perusahaan terhadap jaringan, ada perusahaan yang memiliki keberlangsungan bisnis yang harus dijamin oleh jaringan selama 24 jam penuh, namun ada pula yang hanya pada saat jam kerja saja.

Berikut ini merupakan tabel pengelompokan resiko pada jaringan menurut hasil analisa penulis:

Tabel 4.1 Pengelompokan Resiko Jaringan Hasil Analisa Penulis

No.	Kategori Resiko	Masalah Jaringan
1.	<i>High Risk</i>	a. <i>Host</i> yang memiliki peranan penting tiba-tiba mati, misalkan: router / mikrotik router, <i>DHCP server</i> , <i>Radius server</i> , <i>mail server</i> , <i>DNS server</i> , <i>Proxy server</i> ,

No	Kategori Resiko	Masalah Jaringan
		<p>dan <i>NMS server</i>. status ditunjukkan dengan adanya peringatan <i>Lost Connection</i> atau <i>down</i></p> <p>b. Switch, yang terletak pada bagian DMZ dari jaringan, kemudian yang merupakan bagian dari jaringan backbone ataupun jaringan yang sifatnya <i>crucial</i> dan berpengaruh besar pada jaringan, <i>down</i>.</p> <p>c. Pada jam-jam tertentu, apabila terdapat penambahan daya kerja / utilisasi pada jaringan yang melebihi ambang batas 70%</p> <p>d. <i>traffic</i> pada jaringan yang melebihi ambang batas 70% dari pemakaian biasa</p>
2.	<i>Medium risk</i>	<p>1. Switch dan peralatan layer 2 lainnya yang dicover di dalam jaringan <i>workstation</i> <i>down</i>, masuk kategori medium karena jika rusak masih dapat diakses lewat jaringan <i>workstation</i> lain</p> <p>2. jaringan lambat karena pertambahan user (user login berbeda dari biasanya), utilization antara 40% - 70%.</p> <p>3. UPS mati/ rusak</p> <p>4. Pada beberapa <i>host</i> yang memiliki indikator suhu misalkan router, mengalami peningkatan suhu diatas 50%.</p> <p>5. Voltase pada jaringan yang tidak stabil.</p>
3.	<i>Low risk</i>	<p>Printer dan beberapa peralatan lainnya yang kurang memiliki pengaruh <i>crucial</i> di jaringan, rusak atau <i>down</i></p> <p>Utilization dan beban <i>traffic</i> dibawah 10%</p>

4.2.3. Deskripsi Umum Sistem yang akan Dibangun

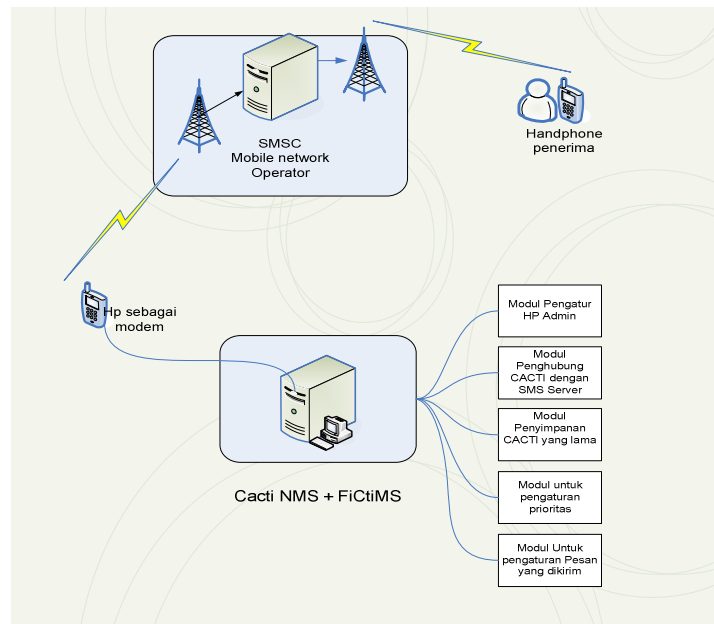
Sistem yang akan dibangun merupakan rancang bangun pengembangan fitur dari sistem yang sudah ada. Pengembangan dan penambahan fitur yang

dimaksud adalah fitur SMS pada CACTI. Fitur ini diberi nama FiCtiMS (Fitur CACTI berbasis SMS).

Rincian penjelasan rancang bangun fitur tersebut dapat dilihat pada penjelasan dibawah ini:

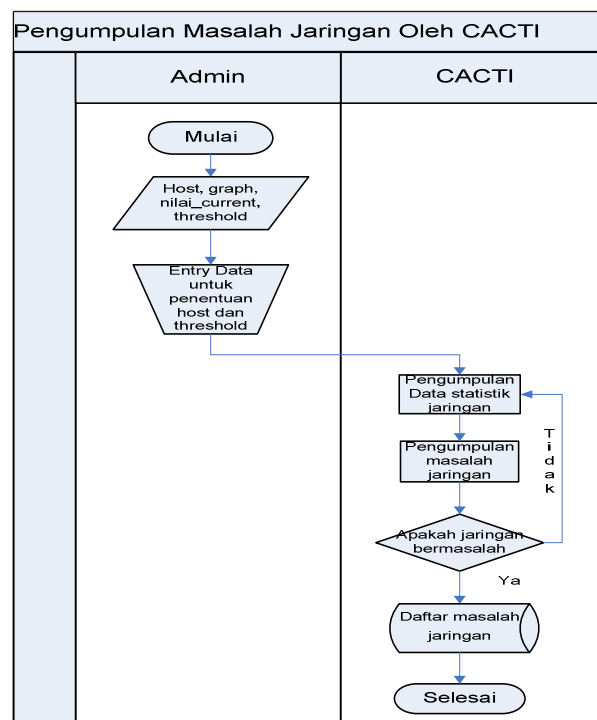
1. FiCtiMS merupakan fitur yang berupa Modul SMS Tambahan yang berisi SMS *gateway* dan program yang menghubungkan CACTI ke program SMS *gateway* itu sendiri
2. CACTI merupakan sistem monitoring jaringan yang bertugas memantau aktifitas jaringan yang kemudian CACTI jugalah yang akan memberikan peringatan bila terjadi masalah pada jaringan
3. Masalah pada jaringan yang dikumpulkan dan disimpan dalam basis data CACTI selanjutnya akan diproses oleh modul SMS tambahan yang kemudian akan dikirimkan menggunakan HP yang berfungsi sebagai modem.
4. SMS peringatan akan diterima dengan segera oleh HP *network administrator* yang tidak sedang berada di tempat. SMS yang diterima merupakan SMS peringatan dengan prioritas tertinggi.

Rancang bangun FiCtiMS secara umum dapat dilihat pada gambar 4.2.



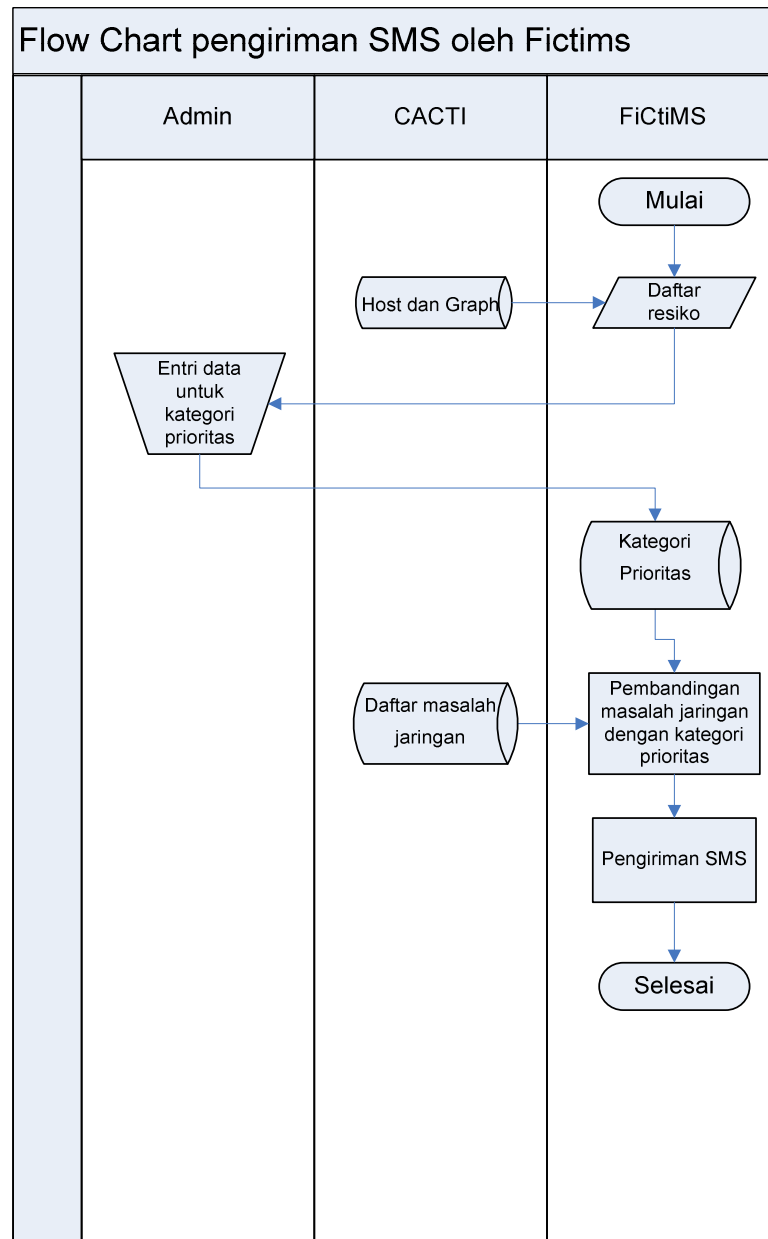
Gambar 4.2 Deskripsi Umum Perangkat Lunak yang akan dibangun

Flow Chart berikut menggambarkan proses pengumpulan data masalah jaringan yang dilakukan oleh CACTI



Gambar 4.3 Proses Pengumpulan Data Masalah Jaringan oleh CACTI

Dan flowchart berikut merupakan proses pengiriman SMS yang dilakukan oleh perangkat lunak yang akan dibangun (FiCtiMS)



Gambar 4.4 Proses Pengiriman SMS pada FiCtiMS

4.2.4. Analisa Perangkat Lunak

Analisa Perangkat Lunak bermanfaat sebagai penentu proses pengerjaan agar ditemukannya suatu pemecahan masalah. Terciptanya keruntutan suatu

analisa perangkat lunak pada jalur yang benar merupakan dasar dilakukannya tahap ini.

Analisa perangkat lunak terdiri atas analisa kebutuhan data, analisa kebutuhan perangkat, analisa kebutuhan fungsi, dan analisa fungsional

4.2.4.1. Analisa Kebutuhan Data

Sesuai dengan metode *priority service* yang digunakan, maka sistem yang akan dibangun memiliki kriteria kebutuhan data sebagai berikut:

- a. Data *host*, berupa IP *host* dan status *host*, ini digunakan untuk menginisialisasi status *host* sekaligus untuk membedakan *host* satu dengan lainnya
- b. Data jenis grafik, berupa grafik template
- c. Nilai ambang batas yang telah ditetapkan pada threshold, nilai data ini bersifat fleksibel karena ditetapkan sendiri ambang batasnya oleh *network administrator* dan akan digunakan sebagai pembanding bagi nilai yang sedang diukur pada suatu waktu

Data-data tersebut telah ada dalam basis data CACTI, sehingga yang akan dibuat adalah membangun *script* yang dapat memanggil data-data tersebut untuk dapat dibandingkan dengan nilai-nilai yang ada pada tabel kriteria prioritas. Dengan demikian, apabila terjadi suatu masalah di jaringan yang dalam hal ini ditandai dengan di langgarnya nilai ambang batas, maka data akan masuk ke data base dan kemudian dibandingkan untuk kemudian akan dikeluarkan sebagai informasi berupa SMS.

4.2.4.2. Analisa Fungsi yang akan dibangun pada Perangkat Lunak

Perangkat lunak ini memiliki beberapa fungsi yang bisa dimanfaatkan oleh user agar dapat menghasilkan output yang maksimal dan berjalan sebagaimana mestinya. Berikut rincian fungsi yang ada didalam fitur yang akan dibangun pada perangkat lunak adalah:

1. Input kategori prioritas
2. Pembandingan nilai basis data CACTI pada suatu waktu dengan nilai input pada kategori prioritas
3. Pengiriman hasil pembandingan pada nomor 2. dalam bentuk SMS
4. Penyimpanan log pesan telah terkirim

4.2.4.3. Analisa Fungsional

Dalam analisa fungsional, aliran informasi yang ditransformasikan pada saat data bergerak dari *input* menjadi *output* dapat dilihat di *Context Diagram* dan *Data Flow Diagram (DFD)*.

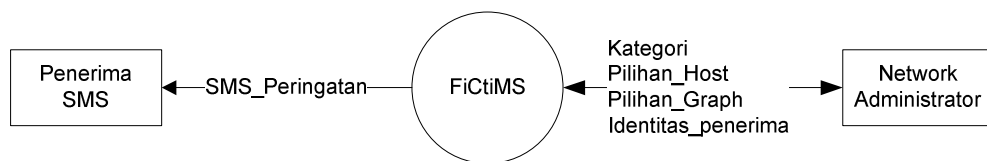
4.2.4.3.1. Context Diagram (Diagram Konteks)

Diagram konteks digunakan untuk menggambarkan hubungan *input* / *output* antara sistem dengan dunia luarnya (kesatuan luar). Suatu diagram konteks selalu mengandung satu proses, yang mewakili seluruh sistem.

Karakteristik entitas yang akan berinteraksi dengan FiCtiMS, yaitu :

- a. *Network Administrator*, bertugas menginputkan kriteria resiko, jenis *host*, jenis *graph* dan identitas penerima SMS. *Network administrator* memiliki hak akses penuh untuk mengatur sistem termasuk manajemen pengiriman SMS. *Network administrator* juga berhak menerima SMS peringatan

- b. Penerima, merupakan entitas yang menerima SMS peringatan permasalahan jaringan. Yang dikategorikan sebagai penerima pesan disini adalah *network engineer* dan orang-orang yang memiliki kepentingan untuk *troubleshooting* masalah jaringan. Yang berhak menentukan penerima adalah *network administrator*, sehingga pada kasus-kasus tertentu *network administrator* juga mendapatkan SMS peringatan.
- c. CACTI, merupakan *tools* yang berguna sebagai sumber data bagi FiCtiMS, yang akan memberi inputan berupa jenis *host*, jenis grafik, nilai status *host* dan nilai ambang batas

Gambar 4.5 *Context Diagram* FiCtiMS**Tabel 4.2 Keterangan Proses *Context Diagram***

No	Nama proses	Masukan	Keluaran	Keterangan
1	Fitur CACTI berbasis SMS	-Kategori -Pilihan_ <i>Host</i> -Pilihan_Graph -Identitas_penerima	-SMS_Peringatan	Proses pada FiCtiMS (Fitur CACTI berbasis SMS)

Tabel 4.3 Keterangan Aliran Data *Context Diagram*

No	Nama	Keterangan
1.	Kategori	Kategori prioritas permasalahan jaringan
2.	Pilihan_ <i>Host</i>	Data <i>host</i> yang dipilih dari tabel <i>host</i> dari basis data CACTI
3.	Pilihan_Graph	Data graph yang dipilih dari tabel graph dari basis data CACTI

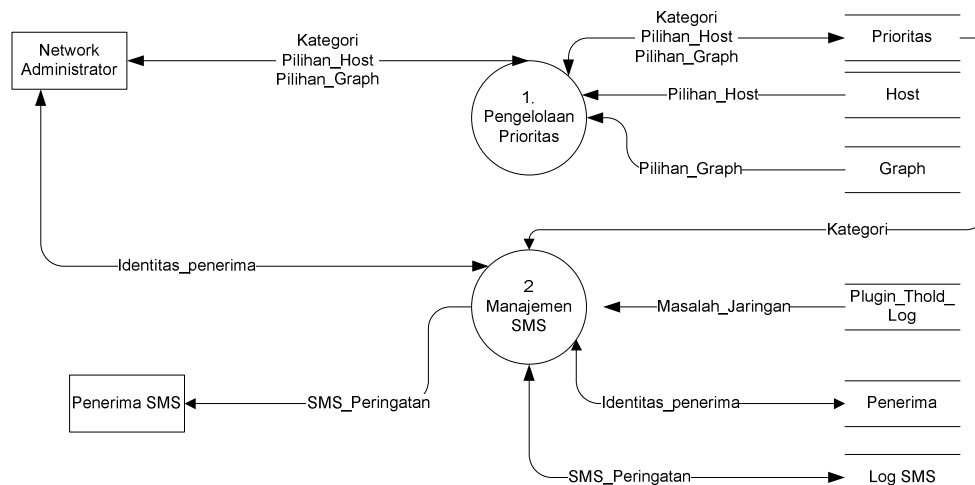
No.	Nama	Keterangan
4.	Identitas_Penerima	Data identitas penerima SMS yang berisi nama dan nomor telepon seluler
5.	SMS_Peringatan	SMS yang berisi peringatan permasalahan jaringan paling prioritas

4.2.4.3.2.Data Flow Diagram (DFD)

Data Flow Diagram (DFD) digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logis tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir.

Perangkat Lunak yang akan dibangun memanfaatkan basis data milik CACTI sebagai penyedia data untuk inputan. *Data store* CACTI yang digunakan sebagai sumber data adalah *data store* Prioritas, *data store* host dan *data store* graph.

DFD level 1 untuk FiCtiMS adalah:



Gambar 4.6 DFD Level 1 FiCtiMS

Tabel 4.4 Keterangan Proses pada DFD Level 1 Proses Pengelolaan Prioritas

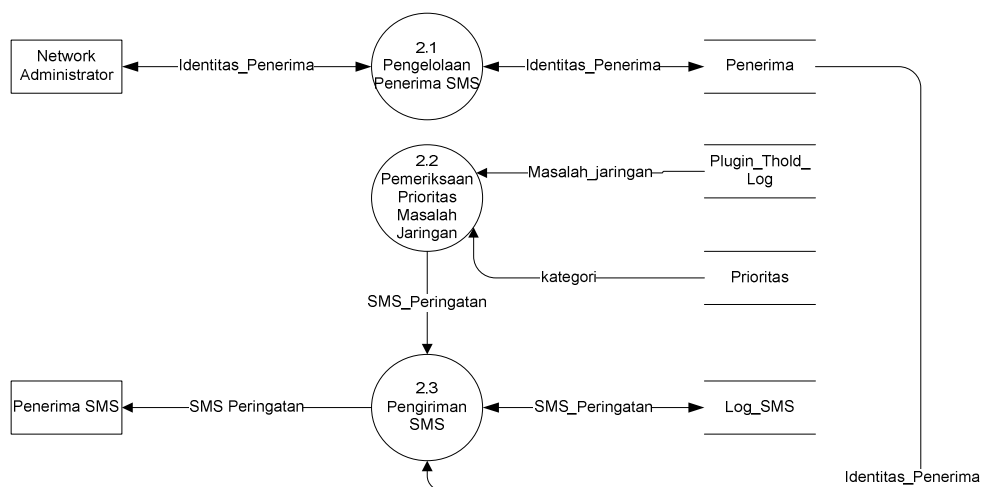
No Proses	1
Nama Proses	Pengelolaan prioritas

Deskripsi	Pengelolaan masalah jaringan berdasarkan prioritas
<i>Input</i>	Kategori, pilihan <i>Host</i> dan pilihan graph
<i>Output</i>	Masuk pada tabel prioritas
Logika Proses	Kategori diinputkan, kemudian pilihan host dan pilihan graph juga diinputkan dengan cara pemanggilan pada <i>data store host</i> dan <i>data store graph</i> pada basis data CACTI

Tabel 4.5 Keterangan Proses pada DFD Level 1 Proses Manajemen SMS

No Proses	2
Nama Proses	Manajemen SMS
Deskripsi	Mengatur penerima, pemeriksaan prioritas masalah jaringan dan mengirimnya sebagai SMS
<i>Input</i>	Identitas penerima, Masalah_Jaringan, dan kategori prioritas
<i>Output</i>	Hasil dari identitas_penerima yang di inputkan, SMS peringatan yang berisi masalah jaringan paling prioritas
Logika Proses	<ul style="list-style-type: none"> -Pengelolaan penerima -Memeriksa data masalah dari <i>data store</i> plugin_thold_log milik basis data CACTI dengan data prioritas dari <i>data store</i> prioritas. Pemeriksaan dilakukan setiap 5 menit sekali, berdasarkan pada poller 5 menit yang telah ditetapkan CACTI -Mengirimkan SMS peringatan kepada penerima

DFD Level 1 proses manajemen SMS mempunyai proses-proses yang lebih kecil. Proses tersebut tertuang pada DFD Level 2 sebagai berikut:



Gambar 4.7 Proses Manajemen SMS

Tabel 4.6 Keterangan Proses DFD Level 2 Proses 2.1. Pengelolaan Penerima SMS

No Proses	2.1
Nama Proses	Pengelolaan Penerima SMS
Deskripsi	Mengelola data identitas penerima
<i>Input</i>	Data Identitas Penerima
<i>Output</i>	Data masuk pada tabel penerima
Logika Proses	Data dikelola kemudian data masuk pada tabel penerima

Tabel 4.7 Keterangan Proses DFD Level 2 Proses 2.2 Pemeriksaan Prioritas Masalah Jaringan

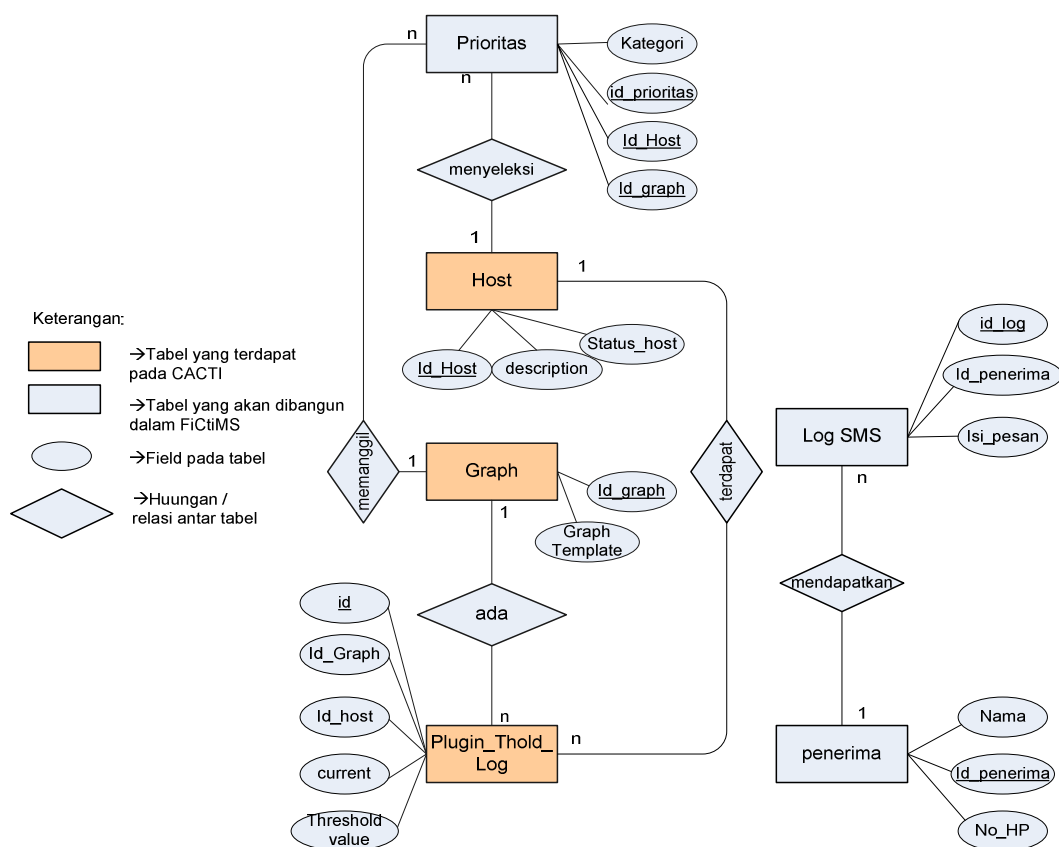
No Proses	2.2
Nama Proses	Pengujian Masalah Jaringan
Deskripsi	Hasil Pengujian data permasalahan jaringan
<i>Input</i>	Data Masalah_Jaringan dari <i>data store</i> Pugin_Thold_Log, data kategori dari hasil pengelolaan prioritas (Proses 2.1) dan data waktu dari tabel waktu
<i>Output</i>	SMS_Peringatan yang siap untuk dikirim
Logika Proses	Setiap 5 menit sekali, sistem akan memeriksa data masalah, data kategori dan data waktu untuk menentukan prioritas masalah jaringan. Data waktu berguna agar tidak terjadi duplikasi pengiriman SMS, sehingga setiap selesai pemeriksaan data dan pengiriman SMS maka data waktu pengiriman pesan akan dibandingkan dengan data waktu dari plugin_thold_log

Tabel 4.8 Keterangan Proses DFD Level 2 Proses 2.3 Pengiriman SMS

No Proses	2.3
Nama Proses	Pengiriman SMS
Deskripsi	Mengirim SMS kepada penerima
<i>Input</i>	SMS_Peringatan siap kirim, Identitas_Penerima
<i>Output</i>	SMS_Peringatan diterima dan tercatat di Log_SMS
Logika Proses	SMS_Peringatan akan dikirimkan kepada penerima sesuai Identitas_penerima, penerima menerima SMS_Peringatan dan sistem mencatat hasil pengiriman pada Log_SMS

4.2.4.3.3.ER-Diagram

ERD (*entity relationship diagram*) berguna untuk mendefinisikan seluruh komponen aliran data dalam sebuah model entitas yang saling berhubungan. Model *entity-relationship* berisi komponen-komponen himpunan *entitas* dan himpunan relasi yang masing-masing dilengkapi dengan *atribut-atribut* yang mempresentasikan seluruh fakta dari "dunia nyata" yang ditinjau. Perancangan ERD tersebut dapat dilihat sebagai berikut:



Gambar 4.8 E-R Diagram pada FiCtiMS

4.2.4.3.4.Data Dictionary (Kamus Data)

Kamus data merupakan keterangan dari *Entity Relationship Diagram* (ERD) yang berisikan nama tabel, atribut dan keterangan masing-masing atribut.

Tabel 4.9 Data Dictionary (Kamus Data)

Nama Tabel	Atribut	Keterangan
Prioritas		Tabel prioritas resiko
	<u>Id_prioritas</u> Kategori <u>Id_host</u> <u>Id_graph</u> status	Id prioritas Kategori resiko Id host Id graph Status host, misalkan down atau mati dan up atau hidup
Log SMS	<u>Id_log</u> <u>Id_prioritas</u> Isi_SMS <u>Id_penerima</u>	Primary key log sms id prioritas Isi SMS terkirim Id penerima sms
Penerima	Nama <u>Id_penerima</u> No_HP	Nama Penerima SMS Primary Key penerima Nomor telepon seluler penerima
Plugin_Thold_Log (dari basis data CACTI)	Time id_Host id_Graph Threshold_id Threshold_value Current status type description <u>id</u>	Keterangan waktu yang menunjukkan kapan masalah jaringan di-trigger Id host Id graph Id threshold/ ambang batas Nilai threshold Nilai sekarang yang berhasil dikumpulkan CACTI Status Log Type Log Deskripsi log Id log (primary key)
Graph (dari basis data CACTI)	<u>Id_graph</u> Graph_template_id	Primary key graph Graph template
Host (dari basis data CACTI)	<u>id_host</u> description status	Primary key host Deskripsi host Status host

4.3. Perancangan Sistem

Tahap perancangan sistem merupakan prosedur untuk mengkonversi spesifikasi logis kedalam sebuah perancangan yang dapat diimplementasikan pada perangkat lunak. Tahap ini dilakukan setelah tahap analisis perangkat lunak selesai dilaksanakan. Perancangan perangkat lunak yang akan dibuat meliputi perancangan Basis Data dan perancangan antar muka yang terdiri dari; perancangan struktur menu dan perancangan tampilan.

4.3.1. Perancangan Basis data

4.3.1.1. Perancangan Tabel

Berdasarkan informasi yang diperoleh dari ER-Diagram, dapat diketahui bahwa akan dibangun 3 tabel sebagai berikut:

4.3.1.1.1. Tabel Prioritas

Identifikasi / Nama : Prioritas

Deskripsi isi : Tabel Prioritas, berisi prioritas resiko yang harus dilaporkan

Jenis : Tabel prioritas

Primary key : id_prioritas

Tabel 4.10 Struktur Prioritas

Field	Type	Length	Attributes	Allow Null	Description
<u>Id_prioritas</u>	int	2	Unsigned	Not null	Id prioritas
Kategori	varchar	20		Not null	Kategori resiko
Id_host	int	8		Not null	Host id, berfungsi sebagai foreign key
Id_graph	int	8		Not null	Graph id, juga foreign key
Status	int	2		Not null	Status host

4.3.1.1.2. Tabel Penerima

Identifikasi / Nama : Penerima

Deskripsi isi : Tabel Penerima SMS Peringatan

Jenis : Tabel penerima

Primary key : id_penerima

Tabel 4.11 Struktur Penerima

Field	Type	Length	Attributes	Allow Null	Description
<u>Id_penerima</u>	int	3	Unsigned	Not null	Id penerima
Nama_penerima	Text	50			Nama penerima
No_HP	Varchar	15		Not null	No HP Penerima

4.3.1.1.3. Tabel Log_SMS

Identifikasi / Nama : Log_SMS

Deskripsi isi : Tabel berisi pesan yang terkirim

Jenis : Tabel Log_SMS

Primary key : id_log

Tabel 4.12 Struktur Log_SMS

Field	Type	Length	Attributes	Allow Null	Description
<u>Id_log</u>	int	4	Unsigned	Not null	Id log pesan terkirim
Id_prioritas	Varchar	50		Not null	Id prioritas
Isi_SMS	varchar	160		Not null	Isi SMS terkirim
Id_penerima	int	3		Not Null	Id penerima

Tabel lainnya (ditunjukkan dengan warna oranye) merupakan tabel pendukung perangkat lunak Tabel-tabel tersebut merupakan bagian dari basis data CACTI, yang akan sangat berguna bagi rancang bangun perangkat lunak FiCtiMS ini. Field yang terdapat pada tabel tersebut serta berguna bagi rancang bangun FiCtiMS dapat dilihat pada penjelasan berikut:

4.3.1.1.4. Tabel *Host*

Identifikasi / Nama : *Host*

Deskripsi isi : Tabel *host* / device dari basis data CACTI

Jenis : Tabel *Host*

Primary key : *id_host*

Tabel 4.13 Struktur *Host*

Field	Type	Length	Attributes	Allow Null	Description
<u><i>Id_host</i></u>	Mediumint	4	Unsigned	Not null	<i>Id host</i> di jaringan
Description	Varchar	150			Deskripsi <i>host</i>
Status	tinyint	2		Not null	Status <i>host</i>

4.3.1.1.5. Tabel *Graph*

Identifikasi / Nama : *graph*

Deskripsi isi : Tabel *graph* milik basis data CACTI

Jenis : Tabel *Graph*

Primary key : *graph_id*

Tabel 4.14 Struktur *Graph*

Field	Type	Length	Attributes	Allow Null	Description
<u><i>Id_graph</i></u>	Mediumint	8	Unsigned	Not null	<i>Id host</i> di jaringan
<i>Graph_template_id</i>	Mediumint	8			<i>Graph template id</i>

4.3.1.1.6. Tabel *Plugin_Thold_Log*

Identifikasi / Nama : *Plugin_Thold_Log*

Deskripsi isi : Tabel daftar Log semua masalah jaringan

Jenis : Tabel Plugin_Thold_Log

Primary key : id

Tabel 4.15 Struktur Plugin_Thold_Log

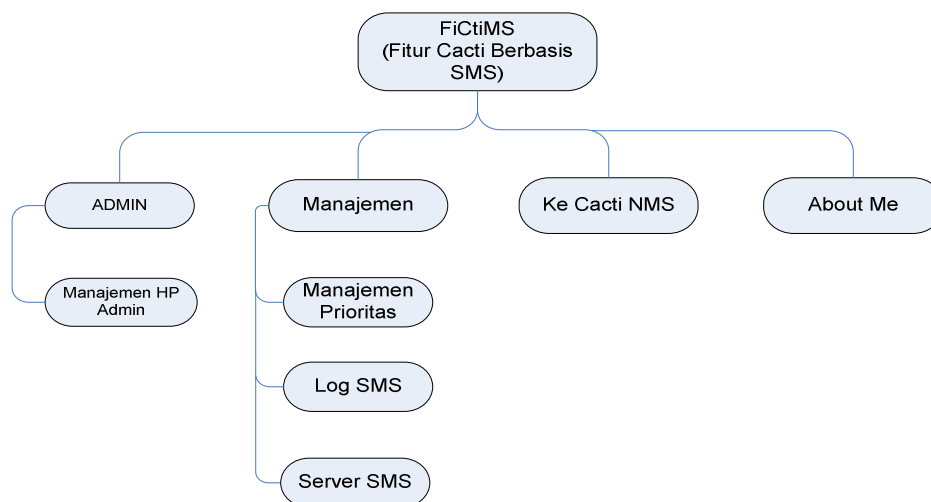
Field	Type	Length	Attributes	Allow Null	Description
<u>Id</u>	int	12	Unsigned	Not null	Id log
Time	int	24		Not null	Waktu trouble
Id_ <i>Host</i>	int	10		Not null	Id <i>host</i>
Id_ <i>Graph</i>	int	10		Not null	Id graph
Threshold_id	int	10		Not null	Id threshold
Threshold_value	varchar	64		Not null	Nilai threshold
Current	varchar	64		Not null	Nilai sekarang
Status	int	5		Not null	Status log
Type	int	5		Not null	Type log
description	varchar	255		Not null	Deskripsi log

4.3.2. Perancangan Antar muka

Perancangan terhadap antarmuka yang akan dibangun merupakan hal yang sangat penting dalam terciptanya kekonsistenan implementasi. Perancangan antarmuka ini terdiri atas dua bagian yaitu struktur menu dan tampilan.

4.3.2.1. Perancangan Struktur Menu

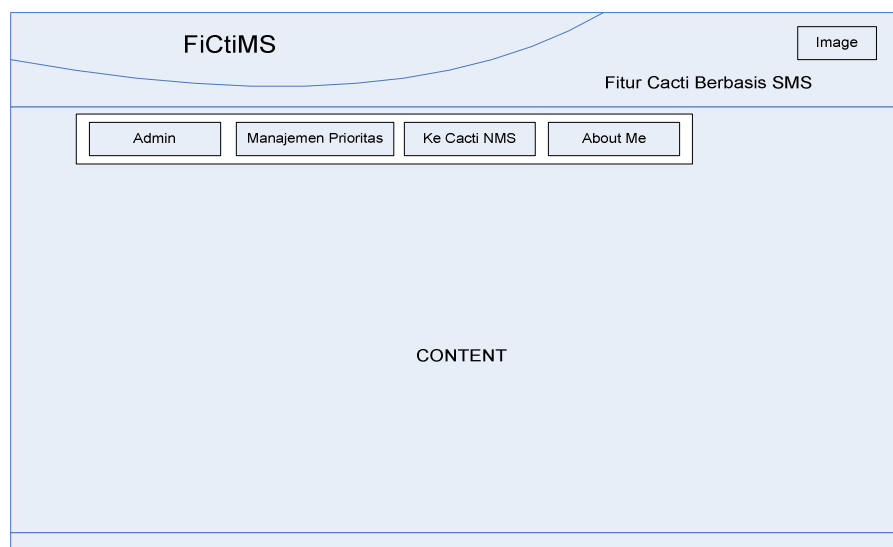
Berikut adalah perancangan struktur menu yang akan dibuat pada FiCtiMS:



Gambar 4.9 Perancangan Struktur Menu

4.3.2.2. Perancangan Tampilan

Berikut adalah rancangan tampilan yang akan dibuat:



Gambar 4.10 Perancangan Antar Muka

BAB V

IMPLEMENTASI DAN PENGUJIAN

5.1. Implementasi Sistem

Implementasi merupakan tahap lanjutan setelah analisa dan perancangan dilakukan. Pada tahapan ini, sistem yang telah selesai, siap untuk dioperasikan dan dilakukan pengujian untuk melihat sejauh mana sistem yang dibuat dapat mencapai tujuan.

Implementasi merupakan kelanjutan dari tahap perancangan sistem yang telah didesain. Pada tahap ini difokuskan kepada penerapan sistem yang didesain pada bahasa pemrograman yang sesuai, sehingga akan diperoleh hasil yang akan diinginkan.

Tujuan implementasi yaitu:

1. Menyelesaikan desain sistem yang ada dalam dokumen perancangan
2. Menguji program-program atau prosedur-prosedur dari dokumen perancangan sistem
3. Mempertimbangkan bahwa sistem sesuai dengan harapan yakni dengan menguji secara keseluruhan.

Langkah-langkah yang dibutuhkan dalam pengimplementasian sistem adalah sebagai berikut.

1. Menyelesaikan desain sistem
2. Memilih Perangkat Lunak
3. Menyiapkan Lingkungan Implementasi

4. Melakukan konversi dari apa yang telah dirancang kedalam bahasa pemrograman (*coding*)
5. Menguji sistem

5.1.1. Alasan Pemilihan Perangkat Lunak

Fitur yang akan dibangun akan menggunakan perangkat lunak berbasis web, yakni PHP, basis data MySQL, DBMS Navicat MySql, Xampp server, mozilla firefox, macromedia dreamweaver MX, dan photoshop CS3. Beberapa pertimbangan digunakannya perangkat lunak tersebut adalah:

1. PHP, MYSQL dan navicat merupakan software yang open source (gratis) dan mampu lintas platform, yaitu dapat digunakan dengan sistem operasi dan web server apapun (windows dan beberapa versi linux)
2. PHP juga merupakan software yang dinamis
3. PHP menawarkan konektifitas yang baik dengan berbagai macam basis data
4. PHP dan MySQL memiliki kecepatan dalam eksekusi perintah dan mampu menangani jutaan request dalam waktu yang bersamaan
5. Navicat mysql lebih user friendly
6. Photoshop CS3 memiliki tools lebih lengkap dibandingkan Photoshop lainnya

5.1.2. Lingkungan Implementasi

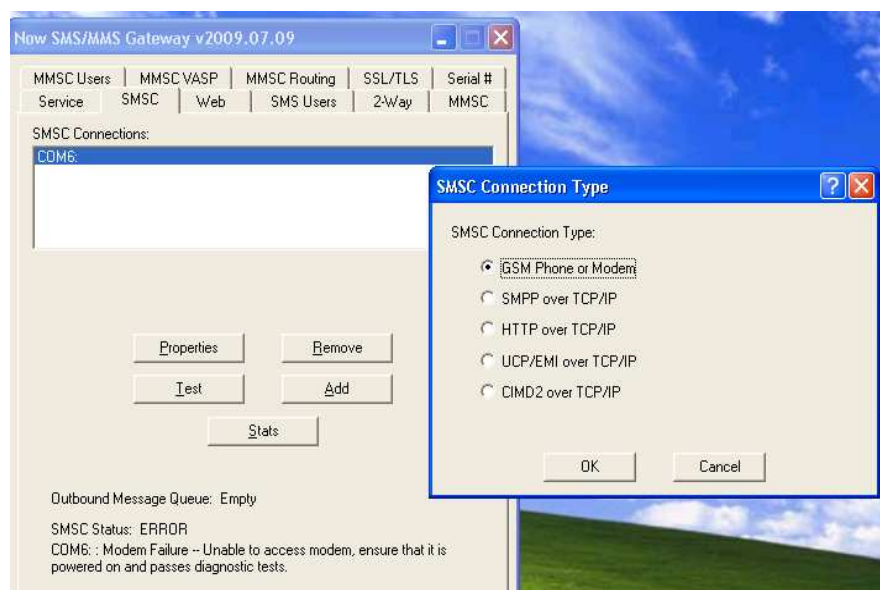
Lingkungan implementasi sistem ada dua yaitu lingkungan perangkat keras (*hardware*) dan lingkungan perangkat lunak (*software*).

1. Perangkat keras (*hardware*)

Perangkat keras yang akan digunakan sebagai tempat untuk instalasi adalah komputer yang memiliki spesifikasi sebagai berikut:

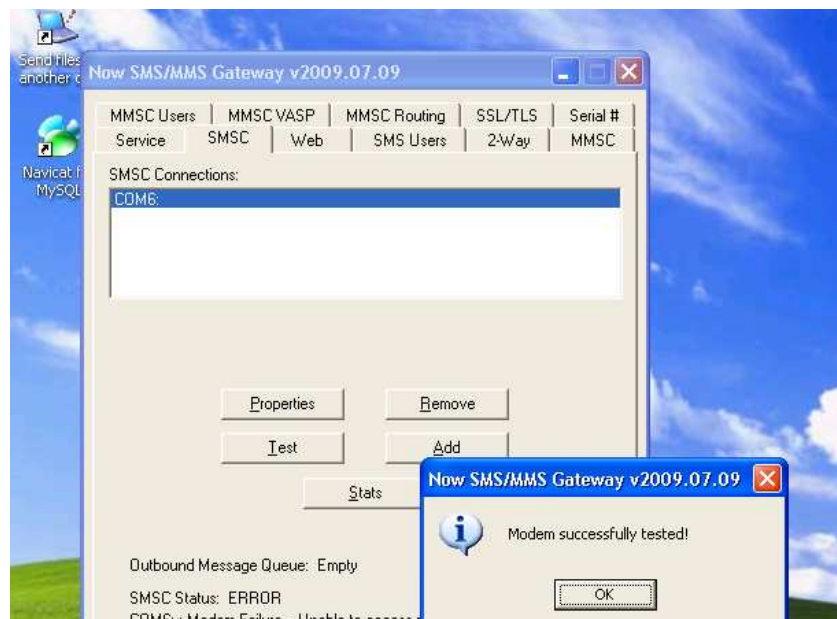
- a. *Processor* Pentium 4 (2,0 GHz)
- b. *Memory* 512 MB
- c. *Hardisk* berkapasitas 40 GB.
- d. Network Interface Card (NIC) / Kartu jaringan

Perangkat keras pendukung yakni modem yang berupa *mobile phone* memiliki spesifikasi yakni HP Nokia Type 6610 dengan kabel penghubungnya dku5. Proses konfigurasi menggunakan NowSMS gateway. Caranya adalah hubungkan port serial pada HP nokia kemudian buka browser NowSMS gateway untuk melakukan konfigurasi. Klik pada banner SMSC untuk mengenalkan port serial HP pada NowSMS gateway. Pilih Com 5 atau Com 6 sesuai yang terdaftar pada port di Device Manager, lihat gambar 5.1. Kemudian lakukan test modem. Jika berhasil akan muncul gambar 5.2.



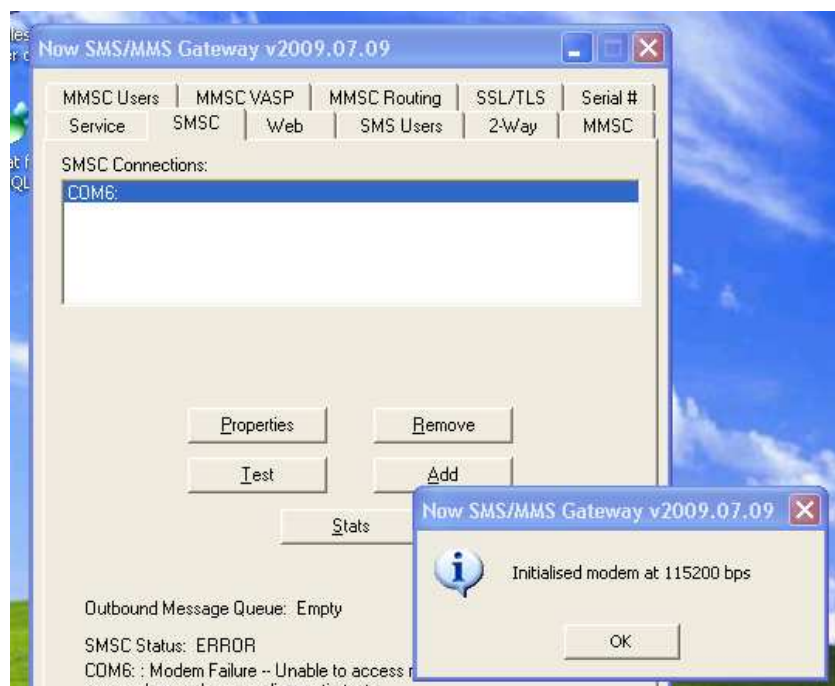
Gambar 5.1 Pemilihan Com untuk Pengenalan Port Serial

Pada pilihan SMSC klik Add maka muncul pilihan koneksi untuk SMSC (SMS center/ pusat pesan). Pilihlah GSM phone or Modem. Setelah itu isilah letak serial COM. Pada contoh diatas adalah menggunakan COM 6. jika pengisian sudah dilakukan klik test modem. Jika berhasil muncul gambar 5.2 dan 5.3



Gambar 5.2 Test Modem berhasil

Klik OK maka akan muncul Gambar 5.3



Gambar 5.3 Inisiasi Modem Pada 115200 bps

2. Perangkat lunak (*software*)

Lingkungan perangkat lunak untuk implementasi aplikasi ini adalah Sistem Operasi *Windows XP*.

5.1.3. Hasil Implementasi

Implementasi dari FiCtiMS menghasilkan beberapa menu untuk mengatur perses pengiriman SMS berisi notifikasi.

5.1.3.1. Menu Admin

Menu admin merupakan menu yang berfungsi untuk mengatur HP yang akan menerima pesan. Pertimbangan untuk meletakkannya pada menu admin adalah karena penerima SMS berkemungkinan adalah bisa admin itu sendiri ataupun orang lain yang ditunjuk untuk melakukan *trouble shooting* jaringan. Menu admin tidak berisi manajemen untuk hak akses karena semua itu sudah diatur secara rinci pada menu utama CACTI.

Dalam manajemen HP, terdapat fasilitas untuk menyimpan, mengubah serta menghapus nama dan nomor HP penerima SMS.



Gambar 5.4 Menu Admin

5.1.3.2. Manajemen Prioritas

Menu manajemen Prioritas merupakan salah satu menu kunci pada perangkat lunak yang dibangun karena proses pengiriman SMS akan berdasarkan pada menu ini. Proses kerja menu ini adalah menambahkan kategori, *host*, *graph* dan status yang ingin dilaporkan. Tersedia juga menu waktu untuk mengatur interval waktu pengiriman SMS alert pada masing-masing kategori. Pilihan *graph* dan status muncul sesuai dengan jenis *host*. Jenis *host* yang berbeda akan memunculkan *graph* yang berbeda pula, tergantung proses pendaftaran pada proses awal CACTI

Daftar prioritas yang sudah ditambahkan akan muncul pada layar. Kemudian, tersedia pula fasilitas untuk mengedit dan menghapus daftar prioritas yang telah ditambahkan.



FiCtiMS

Fitur Cacti Berbasis SMS

Admin Manajemen Menu Utama Cacti About me

Manajemen Prioritas

Data terhapus.

Kategori: High risk
 Host: Localhost
 Graph:
 Status: Any
 waktu: 1 menit
 Simpan

Kategori	Host	Graph	Status

Edit Hapus

Gambar 5.5 Menu Manajemen Prioritas

5.1.3.3. Log SMS

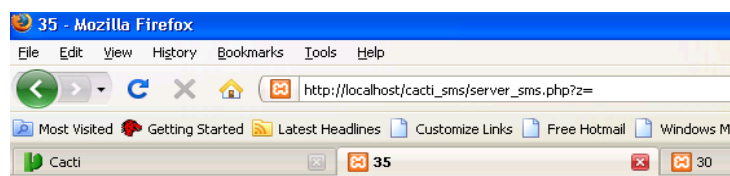
Menu Log SMS berisi pesan/ SMS peringatan yang telah terkirim. Pada prinsipnya, sebelum pesan dikirim akan terlebih dahulu dibandingkan dengan pesan yang ada pada Log SMS untuk menghindari duplikasi pesan terkirim. Kemudian, apabila suatu waktu perangkat jaringan telah diperbaiki dan admin ingin melakukan pengaturan kembali dari awal maka pesan yang terdapat pada Log SMS harus dikosongkan. Proses pengosongan secara otomatis akan dilakukan oleh sistem untuk kondisi jaringan yang telah kembali pulih dari masalah. Namun pada antar muka, disediakan juga fasilitas untuk mengosongkan pesan secara manual seperti yang terlihat pada gambar 5.6.



Gambar 5.6 Menu Log SMS

5.1.3.4. Menu Server SMS

Menu server SMS merupakan menu yang dibuat khusus untuk mengirimkan pesan. Konsep kerjanya adalah ia akan berhubungan langsung dengan table plugin_thold_Log pada basis data CACTI untuk kemudian dibandingkan dengan table prioritas yang telah dibuat sebelumnya pada manajemen prioritas. Hasilnya kemudian dihubungkan dengan Server NowSMS yang akan dikirimkan sebagai pesan. Tampilan menu Server SMS adalah seperti yang terlihat pada gambar 5.7.



Pesan dari status host
7 Host Router Kategori Medium risk+Ket+Down
Pesan sudah masuk di dalam log.

Pesan dari log
1264866575

2010-01-30 22:49:35

Gambar 5.7 Menu Server SMS

Dari gambar terlihat bahwa menu ini berisi pesan yang akan dikirim ke penerima. Pesan-pesan tersebut merupakan hasil perbandingan yang telah dijelaskan sebelumnya.

5.1.3.5.About Me

From ini berisi penjelasan tentang program FiCtiMS secara umum serta cara penggunaannya.



Gambar 5.8 Menu About me

5.2. Pengujian Sistem

Tahap ini merupakan tahap terakhir dari proses pembuatan aplikasi ini. Setelah tahap implementasi dilakukan maka aplikasi harus diuji agar dapat diketahui hasil dari program implementasi sistem. Pengujian dilakukan dengan tujuan untuk menjamin bahwa sistem yang dibuat sesuai dengan hasil analisa, perancangan dan tujuan sebelumnya, juga untuk menemukan kesalahan-kesalahan yang mungkin terjadi sehingga menghasilkan suatu kesimpulan.

Pengujian sistem dilakukan dengan *black box* berfokus dan pengujian akurasi data. Pengujian *black box* berfokus adalah istilah yang digunakan untuk menjelaskan berlangsungnya pengujian saat merancang uji kasus sehingga pengujian tersebut dapat diterima. Pengujian akurasi data adalah pengujian yang dilakukan untuk membuktikan apakah diperoleh kesesuaian data yang dicari secara manual dengan data yang diproses dari sistem. Bila sesuai maka pengujian tersebut telah berhasil.

Keterangan format yang digunakan pada tabel-tabel yang berisikan butir-butir pengujian yaitu:

1. Deskripsi, menerangkan pengujian pada apa yang akan dilakukan
2. Prosedur pengujian, merupakan langkah-langkah untuk melakukan pengujian yang dideskripsikan
3. Masukan, yaitu menginputkan data yang akan diolah
4. Keluaran yang diharapkan, yaitu kesuksesan dari data yang diolah
5. Kriteria evaluasi hasil, yaitu apakah hasil yang diinginkan sesuai dengan keinginan pengguna
6. Hasil yang didapat, menerangkan apakah sistem tersebut berhasil atau tidak
7. Kesimpulan, yaitu diterima atau tidaknya hasil dari pengujian

5.2.1. Kebutuhan Perangkat Uji Coba dan Skenario Pengujian

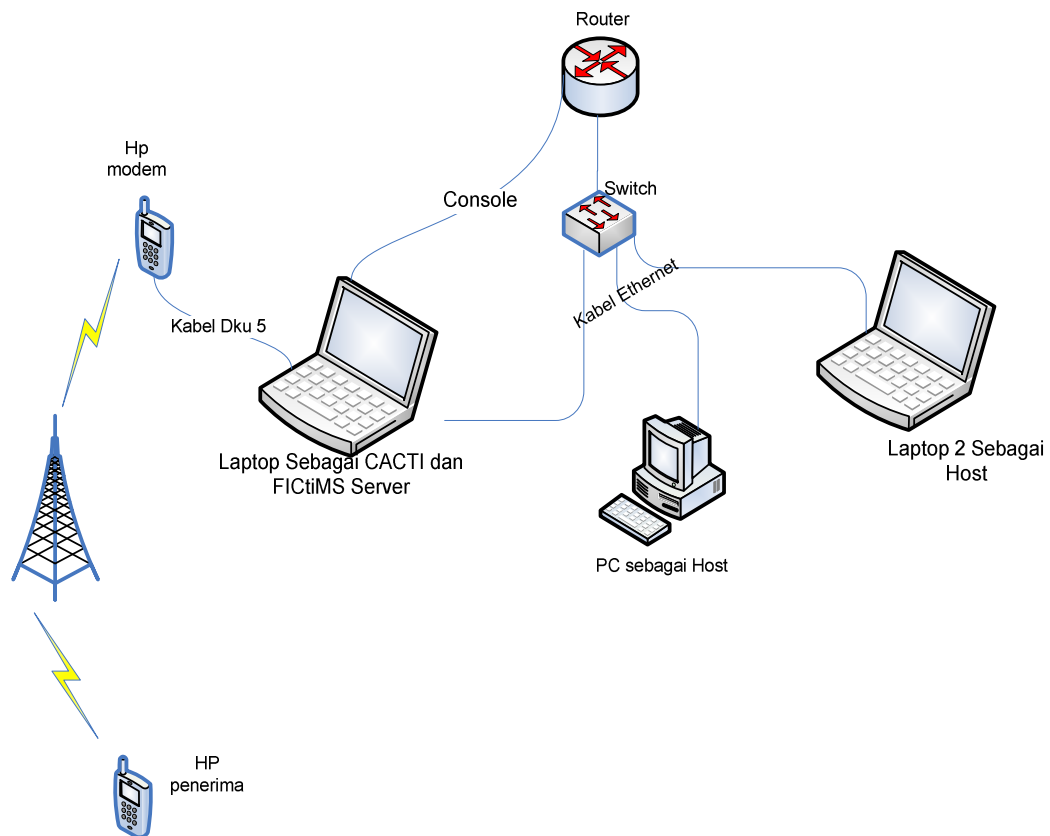
Pada pembahasan analisa, telah disinggung mengenai kriteria prioritas suatu masalah yang terjadi di jaringan. Dalam bahasan ini, akan dipaparkan mengenai kebutuhan perangkat uji coba yang akan digunakan.

Perangkat yang akan digunakan sebagai host untuk uji coba merupakan perangkat keras yang dapat mewakili masing-masing kriteria dari masalah jaringan. Sebagai contoh, sebuah PC yang dapat dianalogikan sebagai server akan mewakili kriteria high risk di jaringan bila nilai status PC tersebut adalah down. Beberapa perangkat lain yang dipakai adalah sebuah laptop dan sebuah router cisco 2600. perangkat tersebut dirasa cukup untuk mewakili masing-masing kriteria resiko permasalahan jaringan. Untuk lebih rinci, berikut analisa perangkat keras yang akan digunakan sekaligus mewakili masing-masing kriteria resiko.

Tabel 5.1 Daftar Prioritas Berdasarkan Host yang Ditunjuk

No	Kategori Resiko	Contoh permasalahan pada masing-masing perangkat
1.	High Risk	<ul style="list-style-type: none"> a. Router, merupakan perangkat jaringan yang <i>crucial</i>. Bila down, termasuk kategori masalah yang <i>high risk</i> b. Begitu pula halnya dengan PC/ laptop yang dianalogikan sebagai server, bila down masuk ke kategori high risk c. Nilai utilization dan aktifitas traffic yang melebihi 70%,bisa dilihat dengan transfer data antar PC dan laptop
2.	Medium Risk	<ul style="list-style-type: none"> a. PC yang dianggap sebagai client, pada jam-jam tertentu apabila memiliki utilization 40-70% maka masuk kategori medium risk b. suhu router lebih dari 50% dari suhu biasa c. penambahan user, dengan melihat <i>login</i> yang aktif pada suatu waktu
3.	Low Risk	<ul style="list-style-type: none"> a. Utilization dari router dibawah 10% b. Lalu lintas traffic dibawah 10%

Berdasarkan penjelasan diatas maka dapat disusun suatu skenario pengujian untuk membuktikan apakah sistem yang dibangun memiliki hasil sesuai dengan yang diharapkan atau tidak. Skenari pengujian tertuang pada gambar 5.9.



Gambar 5.9 Skenario Pengujian

Dari gambar dapat dijelaskan bahwa sebuah laptop akan difungsikan sebagai CACTI server sekaligus FiCTiMS server. Sebuah router, sebuah PC dan sebuah Laptop dipakai sebagai host yang akan diuji. Sebuah HP yang dipasang menggunakan kabel DKU 5 pada laptop berfungsi sebagai modem. Penghubung antara Laptop CACTI dan router adalah kabel *console*, namun dapat juga diganti dengan menggunakan perintah *telnet* dari laptop tersebut.

Pengujian tersebut telah dilaksanakan pada tanggal 25 Januari 2010 di salah satu warung internet di pekanbaru dan 28 Januari 2010 di ruangan dosen Teknik Informatika UIN Suska Riau.

5.2.2. Pengujian Proses Login Pada CACTI Sekaligus FiCtiMS

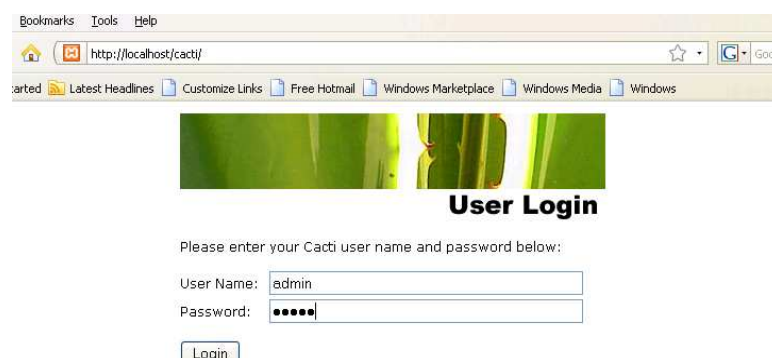
FiCtiMS merupakan fitur CACTI yang fungsi loginnya digabungkan dengan login pada CACTI. Jika login pada CACTI berhasil maka administrator memiliki hak akses penuh terhadap CACTI sekaligus FiCtiMS. Berikut merupakan butir-butir pengujiannya.

Prekondisi : Halaman Awal Login

Tabel 5.2 Butir Pengujian Login CACTI

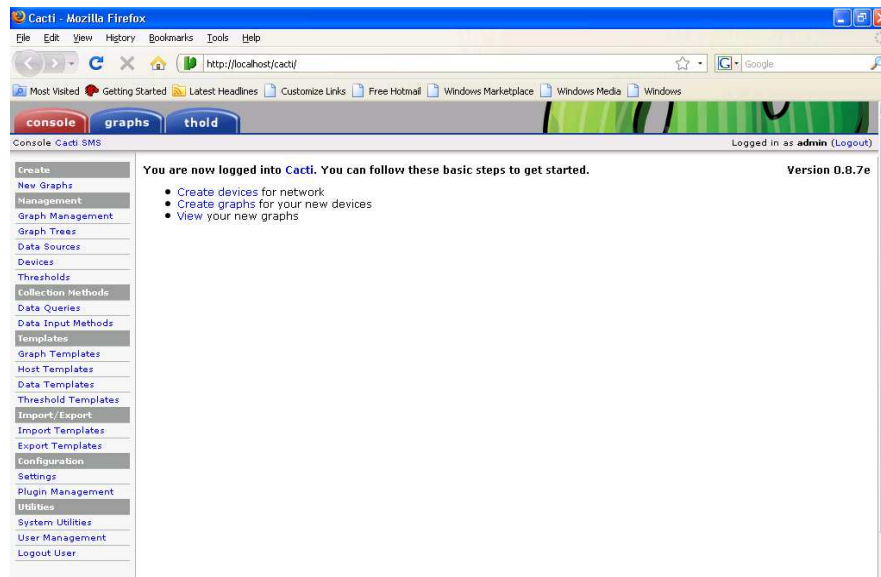
Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian Pendaftaran Graph	1.pada web browser, ketikkan http://: localhost/cacti lalu enter 2.ketikkan username dan password 3.klik menu Cacti SMS	Username dan password	Login CACTI berhasil, dapat mengakses FiCtiMS	Login CACTI berhasil, dapat mengakses FiCtiMS	Login CACTI berhasil. Dapat mengakses CACTI dan juga FiCtiMS	Diterima

Hasil dari pengujian dapat dilihat pada gambar 5.10, gambar 5.11 dan gambar 5.12.



Gambar 5.10 Login CACTI

Tampilan setelah username dan password dimasukkan adalah menu utama CACTI.



Gambar 5.11 Menu Utama CACTI

Pada menu utama CACTI terdapat link ke menu Cacti SMS (FiCtiMS), hasil tampilan setelah menu Cacti SMS di klik adalah gambar 5.12 yakni langsung ke menu manajemen prioritas FiCtiMS.



Gambar 5.12 Menu Manajemen Prioritas FiCtiMS

5.2.3. Pengujian Pendaftaran Host pada CACTI dan THOLD

5.2.3.1. Pengujian Pendaftaran Host

Agar masalah suatu *host* dapat didefinisikan dan dikirimkan, hal paling utama dilakukan adalah mendaftarkan *host* tersebut dalam CACTI. Proses pendaftaran ini nantinya akan memberikan inputan bagi FiCtiMS. Sebagai contoh, mendaftarkan localhost.

Prekondisi : Berada Pada Menu Device (Host belum Terdaftar)

Tabel 5.3 Butir Pengujian Pendaftaran Host

Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian Pendaftaran Host	1. klik link add pada menu <i>device</i> CACTI 2. Masukkan IP host dan deskripsi	Klik Link ADD pada menu Device CACTI	<i>Host</i> berhasil didaftarkan pada CACTI	<i>Host</i> berhasil didaftarkan	<i>Host</i> Terdaftar	Diterima

Untuk hasilnya dapat dilihat pada gambar 5.13.

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Available
iwan	8	9	13	Disabled	1040	192.168.10.10	5.02	5.36	5.28
konoha operator	12	1	1	Disabled	12	192.168.1.3	4.48	24.38	60
localhost	1	9	15	Up	0	127.0.0.1	1045.6	114.29	93.83
PC Joker	4	7	10	Disabled	992	192.168.1.7	20.07	15.47	3.4
PC_Bu_Elin	9	2	4	Down	77	192.168.10.4	3.61	8.06	5.9
Router	7	4	4	Down	77	192.168.10.1	4.66	6.92	7.43

Gambar 5.13 Contoh Hasil Pengujian Pendaftaran Host

Untuk pembuktian yang lebih konkrit bahwa host tersebut telah terdaftar dan terdapat pada aplikasi FiCtiMS dapat dilihat pada gambar 5.14.



Gambar 5.14 Host dan Graph yang Telah Terdaftar dan Dapat Dipilih di FiCtiMS

5.2.3.2. Pengujian Pendaftaran Graph

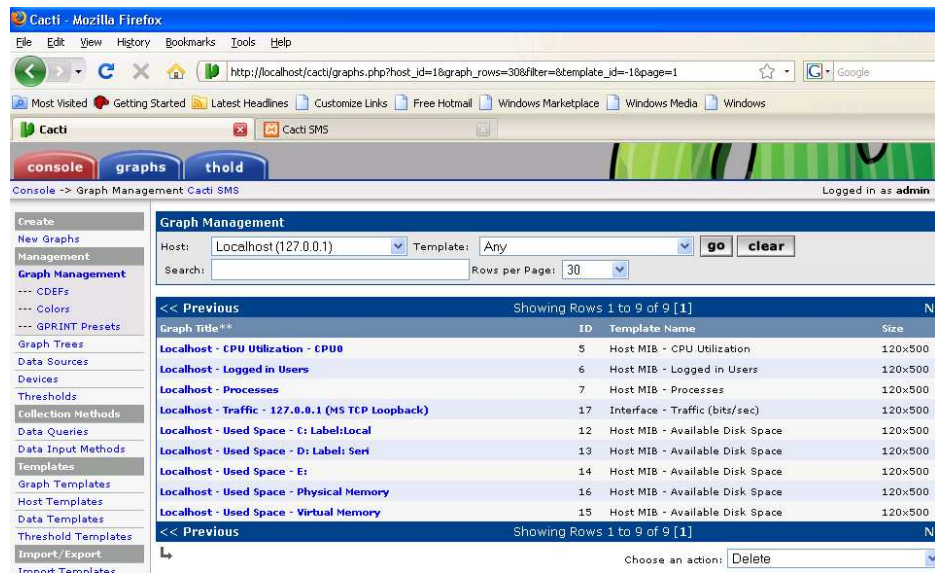
Setelah host didaftarkan, saatnya graph juga didaftarkan.

Prekondisi : berada pada menu Device (Graph belum terdaftar)

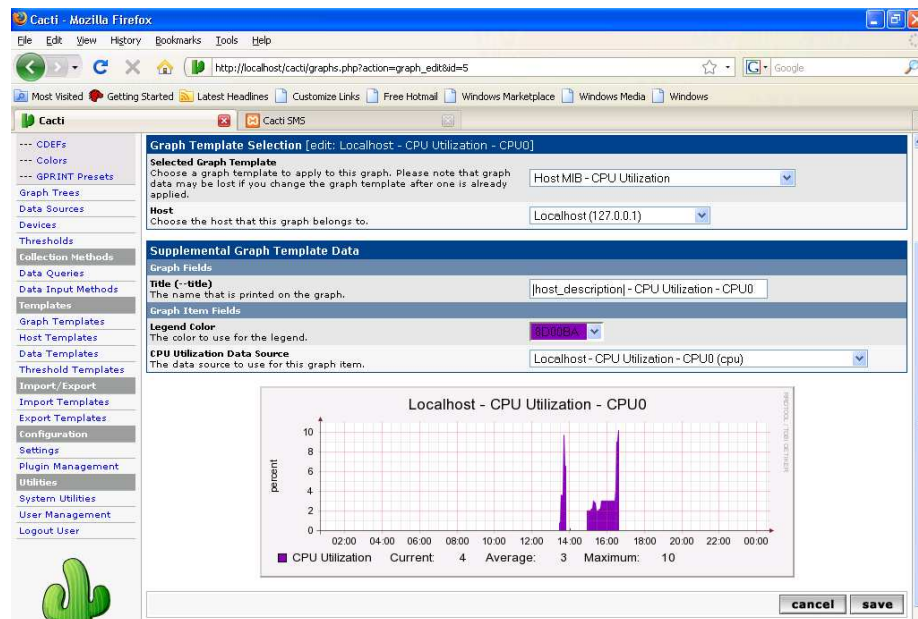
Tabel 5.4 Butir Pengujian Pendaftaran Graph

Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian Pendaftaran Graph	1. Masukkan graph yang ingin dibuat dengan memilih graph template	Pilihan graph template	Graph berhasil ditambah	Graph berhasil ditambah	Graph bertambah	Diterima

Untuk mengetahui hasil uji coba penambahan graph, dapat dilihat pada gambar 5.15 dan 5.16



Gambar 5.15 Hasil Uji Coba Penambahan Graph



Gambar 5.16 Hasil Uji Coba Penambahan Graph Beserta Tampilan Graph

Sama halnya dengan *host*, *graph* yang telah ditambahkan pada CACTI juga akan dapat dimunculkan serta dipilih dari menu manajemen prioritas pada FiCtiMS, lihat gambar 5.14.

5.2.4 Pengujian Pendaftaran *Host* pada Thold

Untuk host yang telah didaftarkan dan telah ditentukan graphnya, jika ingin diketahui permasalahannya haruslah didaftarkan pada Thold. Host dan graph yang telah didaftarkan serta nilai ambang batas yang telah diinputkan akan diproses oleh Thold sebagai parameter penentu masalah jaringan.

Prekondisi : Menu Threshold

Tabel 5.5 Butir Pengujian Pendaftaran Host pada Thold

Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian Pendaftaran Host pada Thold	1. Pilihlah Host dan graph 2. Masukkan ambang batas	Ambang batas	1. Host dan graph terdaftar dalam thold 2. Host dan graph memiliki nilai ambang batas	Host dan graph memiliki nilai ambang batas	<i>Host</i> dan <i>graph</i> terdaftar pada thold dengan nilai ambang batas	Diterima

Hasil pengujian terlihat pada gambar 5.17

Actions	Name**	ID	Type	High	Low	Current	Enabled
	ivan - Traffic - 192.168.10.10/Intel(R) PRO/10 [traffic_out]	3	High/Low	15	1	1663.8333	Disabled
	konoha operator - Processes [proc]	9	High/Low	50	2	54	Disabled
	Localhost - CPU Utilization - CPU0 [cpu]	5	High/Low	10	5	4	Enabled
	Localhost - Processes [proc]	6	High/Low	35	5	42	Disabled
	PC_Bu_Elin - Traffic - 192.168.10.20/Realtek RTL8139 [traffic_out]	10	High/Low	2	0.5	4.2267	Disabled

Gambar 5.17 Hasil pengujian Pendaftaran Host pada Thold

5.2.5 Pengujian FiCtiMS

Pengujian pada fitur CACTI berbasis SMS (FiCtiMS) melalui empat tahapan pengujian yakni pengujian menu manajemen HP, manajemen Prioritas, pengiriman SMS dan pengosongan Log SMS

5.2.5.1 Pengujian Menu Manajemen HP

Prekondisi: tampilan tabel menu manajemen HP kosong

Tabel 5.6 Butir Pengujian Manajemen HP

Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian Manajemen HP	1. Klik menu Admin 2. masukkan nama 3. masukkan nomor HP 4. Klik simpan	Nama dan nomor HP	1. Nama Penerima terdaftar 2. Nomor HP penerima tersimpan 3. Nama dan Nomor HP tampil di layar	Nama dan Nomor HP terdaftar	Nama, nomor HP tampil di layar	Diterima

Hasilnya sama seperti yang terdapat pada gambar 5.18

Gambar 5.18 Pengujian Menu Manajemen HP

5.2.5.2 Pengujian Menu Manajemen Prioritas

Prekondisi : tabel Manajemen Prioritas Kosong/ kategori belum terdaftar

Tabel 5.7 Butir Pengujian Manajemen Prioritas

Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian Manajemen Prioritas	1.klik menu manajemen prioritas 2.masukkan kategori 3.pilihlah jenis host 4.Pilihlah jenis graph 5.pilihlah jenis status 6.masukkan waktu interval 7.simpan	1. Pilihan kategori 2. Pilihan host 3. pilihan Graph 4. pilihan status 5. waktu interval	Kategori masalah berdasarkan prioritas terdaftar dan tampil di layar	Kategori masalah berdasarkan prioritas terdaftar	Kategori prioritas masalah terdaftar dan tampil di layar	Diterima

Untuk melihat hasil pengujian, dapat dilihat pada gambar 5.19

Admin Manajemen Menu Utama Cacti About me

Manajemen Prioritas

Data terhapus.

Kategori: Medium risk
Host: Router
Graph: Cisco - CPU Usage
Status: Up
Waktu: 1 menit

Simpan

Kategori	Host	Graph	Status
High risk	Localhost (1)	Host MIB - CPU Utilization (5)	3
High risk	Localhost (1)	Host MIB - CPU Utilization (5)	1

Edit Hapus

Gambar 5.19 Pengujian Manajemen Prioritas

5.2.5.3 Pengujian Pengiriman SMS

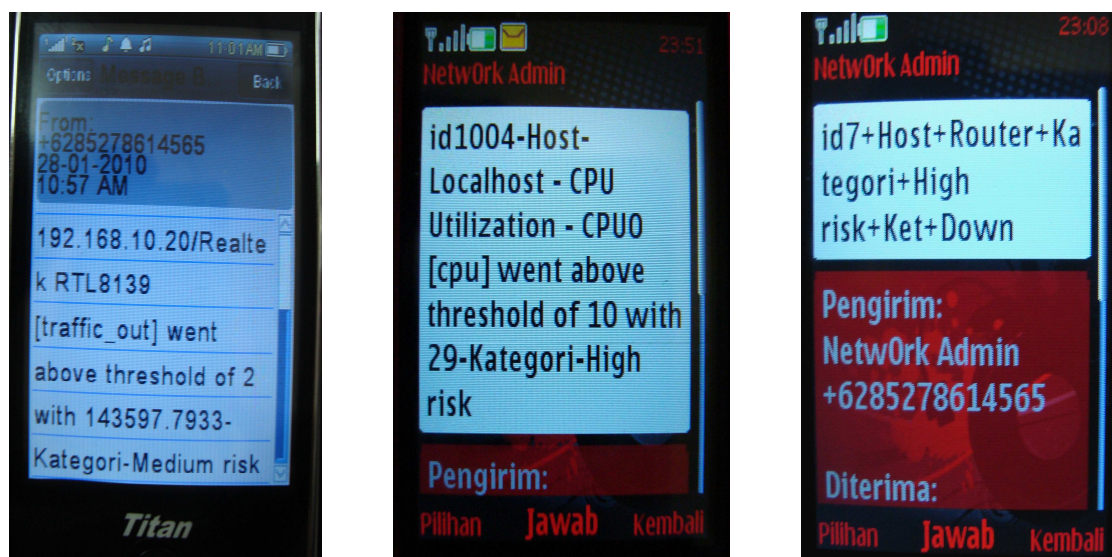
Dalam pengujian pengiriman SMS, terlebih dahulu perangkat HP nokia 6610 dan kabelnya harus terpasang dan terinisiasi dengan benar.

Prekondisi : Belum ada SMS diterima

Tabel 5.8 Butir Pengujian Pengiriman SMS

Deskripsi	Prosedur Pengujian	Masukan	Keluaran yang Diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
Pengujian pengiriman SMS	1.Klik Menu server SMS 2.Cek pada HP penerima apakah SMS sudah diterima	Klik menu Server SMS	SMS masalah sesuai prioritas terkirim dan diterima pada HP penerima	SMS masalah sesuai prioritas diterima pada HP penerima	SMS masalah dikirim, hanya kategori high risk dan medium risk yang dikirim	Diterima

Hasil Pada pengujian pengiriman SMS adalah seperti yang tertera pada gambar 5.20



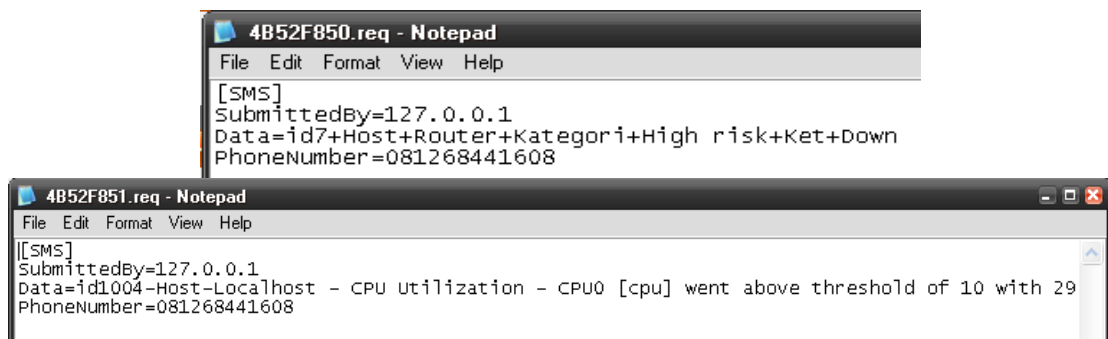
Gambar 5.20 Hasil Pengiriman SMS

SMS yang sudah dikirim dapat dilihat pada log SMS, pembuktiannya dapat dilihat pada Log SMS gambar 5.21.



Gambar 5.21 Pesan yang Sudah Terkirim Masuk Ke Log SMS

Sebenarnya, sebelum SMS dikirimkan kepada HP penerima, SMS tersebut masuk ke daftar antrian milik NowSMS, seperti yang terlihat pada gambar 5.22, perhatikanlah bahwa data pada antrian sama persis dengan SMS yang diterima.



Gambar 5.22 Antrian SMS yang akan dikirim pada NowSMS

5.2.6 Kesimpulan Hasil Pengujian

Setelah dilakukan tahap pengujian terhadap sistem, maka dapat ditarik kesimpulan berkenaan dengan hasil pengujian, yaitu:

1. Network Administrator memiliki hak akses terhadap CACTI dan FiCtiMS sekaligus artinya dengan mengakses CACTI maka network Administrator juga dapat mengaktifkan FiCtiMS

2. Form pengisian data yang terdapat pada aplikasi yaitu : form manajemen HP dan Manajemen Prioritas dapat berjalan sesuai dengan yang diharapkan
3. Sms peringatan berhasil dikirimkan , dan pesan hanya dapat terkirim bila HP penerima didaftarkan
4. SMS terkirim secara otomatis tanpa harus meng-klik tombol refresh setiap saat.
5. Pesan yang terkirim hanyalah pesan dengan kategori High risk dan Medium Risk, Low Risk tidak dikirimkan.

BAB VI

PENUTUP

6.1 Kesimpulan

Berdasarkan pada pembahasan pada Bab-Bab sebelumnya dan merujuk pada tujuan penelitian, dapat diambil suatu kesimpulan yakni:

1. FiCtiMS merupakan fitur baru yang diintegrasikan dalam CACTI untuk mengatasi kekurangan CACTI, fitur ini dapat menyampaikan alert dalam bentuk SMS secara otomatis sesuai dengan interval waktu yang ditentukan
2. FiCtiMS bekerja berdasarkan nilai statistik masalah jaringan yang direkam oleh CACTI untuk kemudian dibandingkan dengan kategori prioritas yang telah dimasukkan pada basis data FiCtiMS, fitur penentuan kategori prioritas masalah jaringan ini dapat diatur secara dinamis
3. Kategori Prioritas merupakan wujud nyata dari implementasi metode *priority service* pada FiCtiMS
4. FiCtiMS belum mampu untuk melakukan monitoring secara *real time*, jadwal poller minimal hanya 5menit sekali dan hanya mampu memonitor hingga layer 3.

6.2 Saran

Aplikasi yang dibangun ini masih memiliki kekurangan, untuk itu pada bagian ini akan dikemukakan beberapa saran untuk perbaikan dan pengembangan, seperti:

1. FiCtiMS hanya mampu untuk mengirimkan SMS searah, fasilitas untuk *trouble shooting* jaringan secara remote belum tersedia sehingga perlu dikembangkan sistem yang mampu mengatasi kekurangan tersebut

2. Perlu diintegrasikan dengan *plugin CACTI realtime* agar dapat memantau jaringan secara *realtime*
3. Untuk mendapatkan informasi pada layer yang berada pada level lebih rendah, terutama layer 1 dan 2 perlu diintegrasikan dengan *tools lspci*
4. Perlu dikembangkan aplikasi untuk mengetahui kondisi sinyal operator dan jumlah pulsa modem secara otomatis

5. mungkin disini, seharusnya: pembagian masalah berdasarkan kategori dan teori prioritas pelayanan, dapat membantu memilah dan mengirimkan masalah berdasarkan kategori prioritasnya. Atau membantu mengatasi masalah pada pemberitahuan notifikasi masalah terhadap admin, mungkin..., tp no 3dah g'da komplain
6. FiCtiMS bersifat dinamis karena kategori permasalahan jaringan dapat ditentukan sendiri oleh Network Administrator sesuai kebijakan yang dimiliki oleh perusahaan
7. SMS terkirim secara otomatis tanpa harus meng-klik tombol refresh setiap saat dan pesan yang terkirim hanya yang memiliki kategori *high risk* dan *medium risk*, kategori *low risk* tidak dikirimkan.

DAFTAR PUSTAKA

- Ahmad, Rivai, "*Bandwidth Monitoring Menggunakan Cacti*" [Online] Available www.geocities.com/ripai Ahmad/bandwidth_monitor_cacti.pdf, diakses 21 September 2009.
- Brenton, Chris ,Cameron Hunt, "*Network security*", *Edisi Bahasa Indonesia Diterjemahkan oleh: Johni Hidayat*. PT Elex Media Computindo, Jakarta: 2005
- "Download Cacti and Plug In" [Online] Available www.cacti.net, Diakses 24 November 2009.
- Ekklesya, "*Network Trouble Shooting*" [Online] Available <http://ekkesya.blogspot.com/2009/12/network-trouble-shooting.html>, diakses 21 Juli 2009.
- Hasan, M. Iqbal, "*Pokok – Pokok Materi : Teori Pengambilan Keputusan*", Ghalia Indonesia, Jakarta: 2002.
- Hendradhy, Oke "Strategi Pengembangan Manajemen Resiko dalam Pengembangan Sistem Informasi" [Online] Available <http://mugi.or.id>, diakses 24 Oktber 2009.
- Hillier, Frederick. S dan Lieberman, Gerald. I, "*Introduction to Operations Research*", Holden Day, Inc. San Francisco:1980.
- "Instalasi Cacti Di mesin *Nix" [Online] Available <http://blidane.wordpress.com/2007/11/21/install-cacti-di-mesin-nix/>, diakses 24 Agustus 2008.
- Jogiyanto, "*Analisa dan Desain Sistem Teknologi Informasi*" Andi Yogyakarta, Yogyakarta: 1999.
- Kakiay, Thomas J, "*Dasar Teori Antrian untuk Kehidupan Nyata*", Andi Yogyakarta, Yogyakarta: 2004.
- Levin, Richard I, dkk, "*Quantitative Approaches to Management (Seventh Edition)*", McGraw – Hill, Inc. New Jersey: 2002.
- "Manajemen Jaringan – Sebuah Tinjauan" [Online] Available <http://noegroz.wordpress.com/2007/07/24/manajemen-jaringan-sebuah-tinjauan/>, diakses 20 Mei 2008.
- Pressman, Roger S, "*Software Engineering: A practitioner Approach*", The McGraw Hill Companies, Inc, New Jersey: 2005.

- Santoso, Beni, “*Membangun Cacti untuk Network Monitoring*”, [Online] Available http://beni-santoso.blogspot.com/2008/02/membangun-cactinetwork-monitoring-di_25.html, diakses 15 Februari 2008.
- Schroeder, Roger G, “*Operations Management*”, McGrawHill, Inc, NewJersey: 1997.
- Siagian, P, “*Penelitian Operasional : Teori dan Praktek*”, Universitas Indonesia Press, Jakarta:1987.
- Spiegel, M. R, “*Teori dan Soal – soal Statistik versi SI (metrik)*”, Alih bahasa : I Nyoman S. dan Ellen G., Erlangga, Jakarta:1988.
- Stalling, William, “*Komunikasi Data dan Komputer Jilid I dan II*”, Salemba Teknika (Cetakan Asli : Pearson Educatin Asia Pte, Ltd), Jakarta : 2002.
- Subagyo, Pangestu, dkk,”*Dasar – Dasar Operations Research*”, BPFE, Yogyakarta: 2000.
- Supranto, Johannes, “*Riset Operasi : Untuk Pengambilan Keputusan*”, Universitas Indonesia Press, Jakarta: 1987.
- Sysneta, “*Standar Keamanan Jaringan Komputer*”, [Online] Available www.sysneta.com/standar-keamanan-jaringan.html, diakses 4 januari 2010
- Taylor, James, “*Managing Information Technology Project*”, AMACOM. Newyork : 2004.
- Team, Cisco, “*SNMP Tutorial*” [Online] Available <http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.pdf>, diakses 9 Juli 2008.
- Terplan, Kornel, “*Communication Network Management, 2nd Edition*”, Prentice Hall. Englewood Cliffs, New Jersey: 1992.
- Tittle, Ed, “*Computer Networking (Jaringan Komputer)*”, alih bahasa : Irzam Hardinsyah, ST, Judul asli : “*Schaum’s outlines of Computer networking*” . PT Elex media Computindo. Jakarta : 2004.
- Walpole, Ronald E, “*Pengantar Statistika Edisi ke – 3*”, Alih bahasa : Ir. Bambang Sumantri, Gramedia. Jakarta:1990.
- Yodi, “*Dasar untuk Membuat Jaringan Komputer yang Aman*” [Online] Available <http://yodi.web.ugm.ac.id> diakses 2 Januari 2010.